Audit Report

MANAGEMENT OF THE JOINT SIMULATION SYSTEM

Report No. D-2002-005

October 12, 2001

Office of the Inspector General
Department of Defense

Report Documentation Page

Report Date 12Oct2001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Management of the Joint Simulation System	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number** D-2002-005
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
Blank page in document

Abstract

We performed this audit in response to a request from the Director, Joint Staff, to evaluate the management of the Joint Simulation System. The Joint Simulation System is a joint training, analysis, and evaluation software tool that will realistically represent the full range of military joint task force operations and provide a synthetic battlefield. The Joint Simulation System was designated an Acquisition Category ID program on December 16, 1999, and is projected to expend nearly $1.55 billion. This is the second audit report on the management of the Joint Simulation System. The first report addressed specific management concerns raised by the Director, Joint Staff. This report addresses the broader topic of overall financial and program management of the development and acquisition of the Joint Simulation System.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU

Number of Pages
45

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DAs	Development Agents
HLA	High Level Architecture
JSIMS	Joint Simulation System
PM	Program Manager
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

October 12, 2001

MEMORANDUM FOR DIRECTOR, JOINT STAFF
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
PROGRAM MANAGER, JOINT SIMULATION SYSTEM

Subject: Audit Report on Management of the Joint Simulation System
(Report No. D-2002-005)

We are providing this report for information and use. We considered management comments on a draft of this report when preparing the final report.

Comments to the draft report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required. In response to the comments, we revised Recommendation 1. to reflect alternative criteria for management corrective action.

We appreciate the courtesies extended to the audit staff. For additional information on this report please contact Mr. Charles M. Santoni, at (703) 604-9051, (DSN 664-9051), csantoni@dodig.osd.mil or Mr. Sean Mitchell at (703) 604-9034, (DSN 664-9034), smitchell@dodig.osd.mil. See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Thomas F. Gimble

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
For Auditing

Office of the Inspector General, DoD

Report No. D-2002-005 **October 12, 2001**
(Project No. D2000AL-0284.01)

Management of the Joint Simulation System

Executive Summary

Introduction. We performed this audit in response to a request from the Director, Joint Staff, to evaluate the management of the Joint Simulation System. The Joint Simulation System is a joint training, analysis, and evaluation software tool that will realistically represent the full range of military joint task force operations and provide a synthetic battlefield. The Joint Simulation System was designated an Acquisition Category ID program on December 16, 1999, and is projected to expend nearly $1.55 billion.

This is the second audit report on the management of the Joint Simulation System. The first report addressed specific management concerns raised by the Director, Joint Staff. This report addresses the broader topic of overall financial and program management of the development and acquisition of the Joint Simulation System.

Objectives. The audit objective was to evaluate the financial and program management of the Joint Simulation System. We also evaluated the management control program related to the objective. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program.

Results. The Joint Simulation System Program Manager has made significant progress toward complying with DoD security and acquisition policies. However, the Joint Simulation System may not receive security certification and accreditation in time for scheduled initial operating capability. Further, the Joint Simulation System acquisition program baselines are not complete or accurate and may not be attainable. As a result, there were no assurances that the Joint Simulation System would provide the level of information technology security required by initial operating capability or that the Milestone Decision Authority would be able to make informed investment decisions concerning the acquisition of the Joint Simulation System.

Summary of Recommendations. We recommend that the Joint Simulation System Program Manager develop an overall security policy in accordance with DS-2610-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001; complete the System Security Authorization Agreement; create a secure trusted environment for the development of the Common Component Workstation; require that the Joint Simulation Development Agents provide complete earned value management information; and construct complete life-cycle cost estimates that include unfunded requirements.

Management Comments. In general, the Joint Simulation System Program Manager concurred with the report recommendations, found many of the draft audit report comments to be accurate, and stated that the Joint Simulation System Program Office will continue to pursue solutions to resolve the problems noted. Management did, however, disagree with specific aspects of the finding and proffered alternative criteria for implementing one of the recommendations. Although management agreed that the

Earned Value Management System has been problematic, they did not agree that there was no assurance that the system will be delivered on time and within budget. The Joint Simulation System Program Manager indicated that other metrics were used in addition to the Earned Value Management System to determine whether costs and schedules were on track, including reviews of planned/delivered source lines of code and planned/delivered functionality for each integration event. The Joint Simulation System Program Manager also stated that there were no unfunded requirements associated with the Joint Simulation System. Further, the Program Manager did not agree that the Joint Simulation System may not receive security accreditation in time for initial operating capability. He stated that there was no obstacle to providing all security documentation prior to system fielding and that there were no known security requirements not currently funded.

The Program Manager stated that the Joint Simulation System security policy had been published and that the system's security procedures manual and security standard operating procedures were being written. Those actions were initiated in accordance with DS-2601-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001, rather than DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997, recommended in the draft report. Funding has been requested to create a secure trusted environment for the development of the Common Component Workstation and corrective actions are ongoing to implement the recommendations addressing the Earned Value Management System and life-cycle cost estimates. A discussion of the management comments is in the Finding section of the report, and the complete text of the management comments is in the Management Comments section.

Audit Response. Management actions with respect to the recommendations are responsive. The report has been revised to incorporate provisions for use of DS-2601-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001, as a basis for developing security policy and documentation. Regarding the management comments on the report findings, we still maintain that there is no assurance that the system will meet cost and schedule goals for initial operating capability. Also, based on recent consultation with the Designated Approving Authority, we still contend that it will be difficult for the Joint Simulation System to obtain security certification and accreditation prior to initial operating capability. Although Joint Simulation System security personnel have made great strides in identifying and documenting those security requirements, significant work still remains to satisfy those requirements.

Table of Contents

Background

The Joint Simulation System (JSIMS), as of April 2001, in system development, is a joint training, analysis, and evaluation software tool that will realistically represent the full range of military joint task force operations and provide a synthetic battlefield. The JSIMS mission needs statement states that:

> The mission of the JSIMS is to provide readily available, operationally valid, computer-simulated environments for use by the Unified Commands, their components, other joint organizations, and the Services to jointly educate, train, develop doctrine and tactics, formulate and assess operational plans, assess warfighting situations, define operational requirements, and provide operational input to the acquisition process.

JSIMS software will be compliant with the High Level Architecture[1] (HLA) in order to support interoperability with other DoD training and analysis simulations. JSIMS software will interface with command, control, communications, computers, and intelligence functions and equipment in the field. It will provide flexible support for joint force training by using efficient, composable simulations tailored to the users' needs. JSIMS will be composed of specific land, maritime, air and space, and other functional domains that will operate in a joint synthetic battlespace. It will create a coherent operational environment between the levels of war, synchronized between types of events, and realistic in the context of the specific joint training scenarios.

JSIMS software will provide the core infrastructure and life-cycle applications to support the effective design, planning, preparation, execution, and post-execution assessment for joint training exercises and other uses. JSIMS will facilitate scenario design, development, and execution by providing tools that systematically link scenario objectives, events, performance measures, and feedback. The Common Component Workstation is a key component of JSIMS because it comprises most of the user interfaces including scenario generation, exercise control, unit control, and evaluation and reporting.

Management and Oversight. On December 16, 1999, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD [AT&L]) restructured JSIMS. The USD (AT&L) designated the Army as the Program Executive Office for JSIMS, and the Commander, U.S. Army Simulation, Training, and Instrumentation Command, as the Program Manager (PM). The JSIMS PM reports directly to the USD (AT&L) with coordination through the Army Acquisition Executive. The JSIMS PM also provides financial reporting to the

[1] HLA is a software architecture structure for major functional elements, interfaces, and design. It pertains to all DoD simulation applications and provides a common framework for the interoperability of simulations, within which specific system architectures can be defined.

Joint Staff. The USD (AT&L) also designated JSIMS, including all of its Service and agency components, as an Acquisition Category ID[2] program and further directed that JSIMS transition to the HLA. The Joint Staff Director for Operational Plans and Interoperability is responsible for the fiscal oversight of the JSIMS common components. The JSIMS PM executes those funds on behalf of the Joint Staff.

JSIMS has nine Development Agents (DAs), each responsible for the development of different aspects of JSIMS. The nine DAs represent each Military Department, the Intelligence Community, and the Office of the Secretary of Defense. The Service DAs are developing JSIMS components that can independently meet the training needs of the respective Services. See Appendix B for a complete list of the JSIMS DAs and a description of their responsibilities.

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence oversees and reviews JSIMS implementation of the Clinger-Cohen Act and DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997.[3]

System Development. JSIMS was designated an Acquisition Category ID program on December 16, 1999. Prior to that date, JSIMS was an Acquisition Category II program, and it was not required to pass milestone reviews conducted by the Defense Acquisition Board. On September 10, 1996, the USD (AT&L) issued a policy memorandum designating HLA as the standard technical architecture for all DoD simulations. The policy required any simulation not compliant with HLA by October 1, 2000, to be retired, unless a waiver was obtained from the Director, Defense Research and Engineering. Although, the JSIMS core development contract was awarded in December 1996, the program did not move toward HLA compliance until USD (AT&L) directed JSIMS management to do so in December 1999, almost 3 years after JSIMS development began.

During our audit, we tried to determine how much money was spent on development efforts that were undertaken after September 1996 and could not transition to the new HLA architecture. Because of the lack of detailed financial information, we could not calculate a complete total. However, we were able to estimate that at least $18.4 million was unnecessarily spent on development

[2] An Acquisition Category ID program is designated by the Under Secretary of Defense for Acquisition, Technology, and Logistics as a Major Defense Acquisition Program, and is estimated to require a total expenditure for research, development, test and evaluation of more than $365 million or, for procurement, of more than $2.19 billion in FY 2000 constant dollars.

[3] DoD Instruction 5200.40 defines the activities leading to security certification and accreditation. The objective of the DoD Information Technology Security Certification and Accreditation Process is to establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure. See Appendix C for more detail.

efforts that could not be transitioned. As certain DAs could not provide any cost data, the $18.4 million estimate may be significantly understated.

The initial deployment blocks of JSIMS software, Block I and Block II, currently in the System Development and Demonstration Phase B of development, are scheduled for a Milestone C, Production and Deployment, Defense Acquisition Board review in September 2002. Partially because of the initial reluctance to use the HLA, the initial operating capability for JSIMS, originally scheduled for December 1999, has been delayed three times, and it is scheduled for March 2003.

Funding. JSIMS is projected to expend nearly $1.55 billion ($1.13 billion in research, development, test, and evaluation funds; $0.18 billion in procurement funds; and $0.24 billion in operation and maintenance funds) from 1996 through 2007. Eight of the DAs are independently funded through respective departments or agencies. The ninth DA is funded directly by the JSIMS PM. The Army is the single largest DA, with a projected budget of $627 million from 1996 through 2007.

Objectives

The audit objective was to evaluate the financial and program management of the JSIMS. We also reviewed management controls as they related to the audit objectives. See Appendix A for a discussion of the audit scope and methodology, the review of the management control program, and prior audit coverage.

Program Performance, Cost, and Schedule

The Joint Simulation System (JSIMS) Program Office has made significant progress toward complying with DoD security and acquisition policies. However, JSIMS may not receive security certification and accreditation in time for scheduled initial operating capability because not all information technology security requirements have been satisfied. In addition, the acquisition program baselines for JSIMS were not complete or accurate and may not be attainable because:

- the JSIMS Earned Value Management System has not provided management with adequate cost and schedule information;
- the JSIMS management has not constructed complete life-cycle cost estimates; and
- there were validated and emerging system requirements for which funding had not been established.

As a result, there were no assurances that JSIMS would provide the level of information technology security required by initial operating capability or that the Milestone Decision Authority would be able to make informed investment decisions concerning the JSIMS acquisition.

Mandatory Guidance

The Office of Management and Budget and DoD provide managers with guidance for acquiring information technology investments and safeguarding information. Appendix C describes the guidance as it relates to the JSIMS acquisition.

Acquisition Category ID Compliance. On December 16, 1999, the Under Secretary of Defense for Acquisition, Technology, and Logistics issued a memorandum designating JSIMS as an Acquisition Category ID program. An Acquisition Category ID program is a Major Defense Acquisition Program subject to review by the Defense Acquisition Board. DoD Instruction 5000.2, "Operation of the Defense Acquisition System," Change 1, January 4, 2001, outlines the documents required for Acquisition Category ID programs. When the audit began in September 2000, required Acquisition Category ID program documents such as the acquisition strategy, the test and evaluation management plan, and the risk management plan did not exist. Further, the JSIMS program was not in compliance with the information technology acquisition requirements of the Clinger-Cohen Act, that requires economic analysis, performance measures, business process reengineering, and an information assurance strategy. Specifically, the JSIMS PM had no documentation regarding JSIMS compliance with the Clinger-Cohen Act.[4] During the course of the audit, the new JSIMS

[4] The Clinger-Cohen Act governs the acquisition of information technology, which requires Chief Information Officer monitoring of system acquisition and the establishment of performance measures

management team worked diligently to generate the documents needed to comply with DoD policy and congressional direction. Although some of those documents were not finalized, the JSIMS PM has made every effort to adhere to DoD policy, and he is making significant progress towards attaining compliance, thereby reducing our concerns in those areas. However, JSIMS and its Common Component Workstation will have a difficult time obtaining system security certification and accreditation. Further, several factors may impact the attainability of JSIMS cost and schedule objectives.

JSIMS Information Technology Security Certification and Accreditation

Prior to March 2000, the JSIMS Program Office did not take action to comply with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997 or with the DS-2610-142-01, "DoD Intelligence Information System Security (DoDIIS) Certification and Accreditation Guide," April 2001. Since that time, the JSIMS PM has made significant progress towards complying with those requirements; however, a considerable amount of work remains to attain system security certification[5] and accreditation[6] for JSIMS and its Common Component Workstation. Additional obstacles that need to be overcome include the approval of the System Security Authorization Agreement.

Security Certification and Accreditation of JSIMS. The JSIMS may not attain security certification and accreditation for Version Release Module 1, scheduled for March 2002; Milestone C, Production and Deployment, scheduled for September 2002; or for initial operating capability currently scheduled for March 2003. JSIMS interacts within a complex environment, including the Intelligence Community, which heightens concern over system security. Intelligence Community personnel identified the following concerns that increase the risk associated with JSIMS security:

- lack of a completed system security procedures manual;
- prior involvement of foreign nationals in JSIMS software development, especially in the Common Component Workstation and the Synthetic Natural Environment;
- lack of a breakdown of specific responsibility for JSIMS system security;

regarding progress towards meeting program objectives.

[5] Security certification is a comprehensive evaluation of the technical and non-technical security features of an information technology system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

[6] Accreditation is a formal declaration by the Designated Approving Authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

- lack of a developed set of rules for the dissemination of secret collateral intelligence across the run time interface; and

- lack of a full understanding of how different software systems developed by different contractors and DAs interact.

The decentralized management of JSIMS, and the perception by the JSIMS PM and DAs that JSIMS is just a training system, resulted in security receiving minimum attention prior to the December 1999 reorganization directed by the Under Secretary of Defense for Acquisition, Technology, and Logistics. Beginning in March 2000, the JSIMS PM made system security certification and accreditation a major priority. However, JSIMS will have a difficult time achieving certification and accreditation by March 2003.

System Security Authorization Agreement Criteria. The purpose of the System Security Authorization Agreement, required by DoD Instruction 5200.40, is to address each of the security items detailed in the Security Requirements Traceability Matrix. The DS-2610-142-01 DoDIIS Security Guide also contains such requirements. Therefore, the agreement should contain all the information necessary for the collateral Designated Approving Authority, the sensitive compartmented information Designated Approving Authority, and ultimately, the system Designated Approving Authority to make a decision regarding the approval to operate the system. It is a formal agreement between the system PM, the Designated Approving Authority community, certification authorities, and user representatives. The agreement is used throughout the certification process to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational system security.

System Security Authorization Agreement Developed for JSIMS. The JSIMS PM has made enormous progress in developing the System Security Authorization Agreement since our initial visit. However, the System Security Authorization Agreement was not complete enough to obtain accreditation and certification and did not satisfy the minimal requirements of DoD Instruction 5200.40 or the DS-2610-142-01 DoDIIS Security Guide. The System Security Authorization Agreement, prepared by the JSIMS Program Office using the DS-2610-142-01 DoDIIS Security Guide, did not include the following topics, completed in a manner acceptable to the Designated Approving Authority, as required for system accreditation:

- data flow (including data flow diagrams),
- security environment,
- IT system characteristics,
- roles and responsibilities, and
- personnel and technical security controls.

We informed the Designated Approving Authority of the incomplete sections of the JSIMS System Security Authorization Agreement and he agreed that the information associated with those sections is needed for system certification and accreditation. Because JSIMS has a decentralized management structure, eight of the nine DAs act independently and provide their own funding. If the required sections or acceptable alternatives are not adequately documented in the System Security Authorization Agreement, the DAs may not have a clear definition of what they are expected to do to ensure the success of JSIMS.

Certification and Accreditation Approval for the Common Component Workstation. The JSIMS Common Component Workstation software will operate in two security domains. One is an upper security enclave that processes top secret and sensitive compartmented information, and the other is a lower security enclave that processes data at the secret level and lower. Early in the JSIMS development stage, the JSIMS PM did not design security measures into JSIMS and the PM did little to address security until March 2000. The Common Component Workstation software was not constructed in a trusted environment[7] because the PM for the Warfighting Simulation System, tasked with developing the Common Component Workstation, did not provide proper instructions to the contractor. Further, the System Security Authorization Agreement does not include the information necessary for the JSIMS Common Component Workstation software development to meet certification and accreditation requirements. The JSIMS PM will have difficulty addressing those security issues prior to the established initial operating capability date.

The National Reconnaissance Office is developing a user interface tool that will allow secure operations if the Common Component Workstation does not receive accreditation. It is coordinating the development with the Warfighters' Simulation Intelligence Module and the Defense Intelligence Agency Object Oriented Model of Intelligence Operations. Personnel within the National Reconnaissance Office stated that they developed the user interface tool because they have no confidence that the Common Component Workstation will be certified by Version Release Module 1.

Cost and Schedule

Several factors may negatively impact the JSIMS cost and schedule. We determined that the JSIMS Earned Value Management System does not provide management with adequate cost and schedule information. Also, the JSIMS Program Office has not constructed complete life-cycle cost estimates and has not included additional security requirements and emerging requirements in the life-cycle cost estimates or budgets. Further, the Army Threat System Management Office has not completed a JSIMS System Threat Assessment Report.

Earned Value Management System. DoD Regulation 5000.2-R (Interim), "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs,"

[7] A trusted environment is an environment where software is constructed by U.S. personnel who are cleared to the secret level and who work in a facility cleared for secret information.

January 4, 2001, (finalized on June 10, 2001) states that the PM will obtain integrated cost and schedule performance data to monitor program execution. PMs must require contractors to develop and use internal management control systems that:

- produce data indicating work progress,
- properly relate cost,
- identify schedule and technical accomplishment,
- are valid, timely and auditable, and
- provide DoD PMs with summarized information.

Data will be compiled and reported in accordance with the Earned Value Management System, unless the contract is valued at less than $73 million, in which case the data may be compiled in alternative ways. In response to this requirement, the JSIMS PM instituted an earned value reporting system that required each DA to provide earned value information to the JSIMS PM on a monthly basis.

The JSIMS PM compiles the data from the various DAs into a central, monthly earned value report that is intended to provide the JSIMS PM with information that indicates whether the program is meeting cost and schedule goals. However, the earned value data compiled by the JSIMS PM are incomplete and unreliable. The most current earned value report as of March 2001 was produced in January 2001. The January report included outdated data for the National Reconnaissance Office and the United States Marine Corps portions of JSIMS. Although the Defense Intelligence Agency provided data for its portion of JSIMS for December 2000 and January 2001, it did not provide data prior to that period. Also, although the reports appear to show that the National Security Agency portion of JSIMS is both on schedule and on target for cost, National Security Agency personnel advised their Earned Value Management System for this contract was not based on planned work. This contract was rebaselined in April 2001 and the contract will begin reporting actual performance indices. Personnel from the Air Force stated that the current prime development contract for their portion of JSIMS does not require the contractor to provide earned value information. However, the contractor has been providing the earned value information to the PM. The Air Force data indicate that the Air Force portion of JSIMS is about 2 percent behind schedule and 1 percent under cost. The Air Force stated that a planned rebaselining of the contract will ensure that the appropriate Earned Value Management System requirements are stated.

As of January 2001, the Navy portion of JSIMS reported 7.6 percent behind schedule. The Army portion of JSIMS reported 3.7 percent behind schedule and 3.8 percent over cost. The earned value documents imply that in order for the Army portion to meet the delivery date for Version Release Module 1.0 (March 2002), some requirements originally intended to be satisfied with Version Release Module 1.0 will be deferred to later versions of JSIMS. A more detailed review of the variances associated with specific aspects of the Army portion of JSIMS revealed that the software development was actually $4.8 million (14 percent) over the projected cost. The JSIMS PM noted that the Army has met its delivery dates for JSIMS integration events including planned delivery of source lines of code and associated functions. The insufficient earned value reports, coupled with the Army and Navy negative schedule variances, provided no assurance that the

JSIMS program would be delivered on time for scheduled initial operating capability and within budget. Furthermore, because of the incomplete nature of the earned value reports, the JSIMS PM could be caught unaware of cost and schedule variances that might materially impact JSIMS.

Also, the various DA earned value reports reflect the schedule status based on internal DA schedules and not the overall JSIMS schedule. Earned value reports have no notation as to how the particular DA schedule relates to the overall JSIMS schedule. Therefore, although an earned value report may indicate that a particular DA portion of JSIMS is behind schedule, it does not necessarily mean that the overall JSIMS schedule is impacted. The JSIMS PM stated that the DA reports should note how a variance effects the overall JSIMS integration events. However, the reviewed reports contained no documentation to indicate how the integration events were impacted. Although the JSIMS PM expressed confidence that JSIMS will be delivered on time and within budget, the Earned Value Management System for JSIMS provides no such assurance.

Life-Cycle Costs. DoD Regulation 5000.2-R (Interim) requires, for reporting purposes, the PM life-cycle cost estimate as defined in DoD 5000.4-M, "Cost Analysis Guidance and Procedures," December 1992. DoD Regulation 5000.2-R (Interim) also requires that every acquisition program establish program goals, thresholds, and objectives for the minimum number of cost, schedule, and performance parameters that describe the program over its life cycle. DoD Regulation 5000.2-R (Interim) defines affordability as "the degree to which the life-cycle cost of an acquisition program is in consonance with the long-range investment and force structure plans of the DoD or individual DoD Component." The PM is required to prepare a life-cycle cost estimate for all Acquisition Category I program initiation decisions and at all subsequent program decision points.

DoD Regulation 5000.2-R (Interim) also requires that the estimating activity explicitly base the life-cycle cost estimate on program objectives, operational requirements, contract specifications, careful risk assessments, and a DoD program work breakdown structure for Acquisition Category I programs. The life-cycle cost estimate must be comprehensive to include all cost elements, such as operation and support costs, that affect the decision to proceed with development or production of the system, regardless of funding source or management control. In addition, DoD Regulation 5000.2-R (Interim) requires the PM to base software systems design and development on systems engineering principles that:

- elect the programming language in context of the systems and software engineering factors that influence overall life-cycle costs, risks, and the potential for interoperability; and

- consider embedded training and maintenance techniques to enhance user capability and reduce life-cycle costs.

The JSIMS PM and the DAs are constructing life-cycle cost estimates scheduled for completion during the summer of 2001. The JSIMS PM and the DAs did not have life-cycle cost estimates that identified complete JSIMS costs. The JSIMS PM and the DAs did not construct cost estimates beyond FY 2007, even though the system has an estimated life through 2022.

Unfunded Requirements. Certain security requirements and validated and emerging program requirements, not accounted for in the JSIMS budget, need to be included in JSIMS life-cycle cost estimates. During the audit, three of the DAs expressed concerns about unfunded requirements for their portion of the JSIMS development. The Defense Intelligence Agency had the most significant unfunded requirement for an additional $35.5 million from FY 2002 through FY 2007, that is needed to provide the complete minimum essential functionality approved by the JSIMS Joint Requirements Control Board. The unfunded requirement included increased automation of organizational behavior and analysis fusion, support for dissemination of imagery and video products, and several other capabilities that would result in a reduction in intelligence personnel needed to support exercises. The JSIMS PM denied that this is an unfunded requirement; however, DIA recorded it as such.

Managers for the Army portion of JSIMS claimed that an additional $11.0 million was needed between FY 2001 and FY 2007, including $4.4 million for additional software development. A component of the Air Force portion of the JSIMS required an additional $1.5 million from FY 2002 through FY 2006. The Air Force recognized that functionality was otherwise jeopardized, and it acknowledged the shortfall and intends to provide the needed funds. Managers for the Navy portion of JSIMS described their funding as uncertain because of emerging requirements. Navy personnel were unable to calculate the amount of funding that will potentially be needed to satisfy its emerging requirements if validated. The JSIMS PM believed there were no unfunded requirements because the JSIMS PM used cost as an independent variable. The JSIMS PM would complete as many requirements in the Operational Requirements Document as funding permits.

System Threat Assessment Report. As of April 2001, a JSIMS System Threat Assessment Report has not been completed. A System Threat Assessment Report describes the threat that a particular system is projected to encounter during its service life. The JSIMS System Threat Assessment Report is being developed by the Threat System Management Office in Huntsville, Alabama, and it is scheduled to be completed between June 2001 and September 2001. Once completed, the threat assessment report has to be validated by the Defense Intelligence Agency. Because this document was not developed prior to the JSIMS development effort, it is possible that JSIMS may not have addressed key projected system threats. If validated threats are identified that JSIMS needs to be protected against, additional costs and delays may be incurred.

Summary

Historically, JSIMS has had problems that have resulted in schedule delays and increased costs. The new JSIMS management team has made significant progress toward correcting various identified problems. Although the JSIMS PM has made extensive inroads to address system security certification and accreditation issues, JSIMS and the Common Component Workstation will have a difficult time obtaining system security certification and accreditation prior to initial operating capability. The JSIMS PM needs to initiate action to create a trusted environment for development of a Common Component Workstation. The JSIMS PM also needs to complete all minimally required sections in the System Security Authorization Agreement. Finally, the lack of a reliable Earned Value Management System coupled with potential unfunded requirements, leave the JSIMS Program continually vulnerable to additional negative cost and schedule impacts and reduced system capabilities. As a result, there are no assurances that JSIMS will provide the level of information technology security required by initial operating capability or that the Milestone Decision Authority will be able to make informed investment decisions on the JSIMS acquisition.

Management Comments on the Finding and Audit Response

Program Office, Joint Simulation System Comments. The JSIMS PM stated that he generally found many of the audit comments to be accurate, and he indicated that the JSIMS Program Office would continue to pursue solutions to resolve the problems noted. However, management disagreed with certain specific aspects of the Finding. Management agreed that the Earned Value Management System has been problematic, but did not agree that there was no assurance that the system would be delivered on time and within budget. The PM indicated that other metrics were used in addition to the Earned Value Management System, to determine whether costs and schedules were on track, including reviews of planned/delivered source lines of code and planned/delivered functionality for each integration event. The PM also stated that there were no unfunded requirements associated with JSIMS. Further, the PM did not agree that JSIMS may not receive security accreditation in time for initial operating capability. He stated that there was no obstacle to provide all security documentation prior to system fielding and that there were no known security requirements that were not funded. See the Management Comments section of the report for a complete text of the management comments.

Audit Response. We still maintain that there is no assurance that JSIMS will meet cost and schedule goals for initial operating capability and that not all requirements are documented and funded. Despite the use of a variety of metrics, the JSIMS PM is required to institute an accurate and complete Earned Value Management System. Also, based on recent consultation with the Designated Approving Authority, it will be difficult for JSIMS to obtain security certification and accreditation prior to initial operating capability. Even though the JSIMS security personnel have made great strides in identifying security requirements both during the audit and since the completion of our audit field work, significant work still remains to satisfy those requirements. In some cases, the JSIMS PM disagreed with details in the audit report, not because the details were inaccurate, but because corrective actions had been initiated or completed since the end of our audit field work. We believe that our report was accurate at the time the field work was completed, and we credit the JSIMS PM for initiating prompt corrective action.

Recommendations, Management Comments and Audit Response

In response to management comments on the draft of this report, Recommendation 1. was revised to reflect adherence to DS-2610-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001 rather than DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997.

1. We recommend the Joint Simulation System Program Manager in accordance with DS-2610-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001:

a. Develop an overall security policy, including a security procedures manual, and system security requirements;

b. Include all sections required by DS-2610-142-01 "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001 in the System Security Authorization Agreement; and

c. Create a secure trusted environment for developing the Common Component Workstation;

2. We recommend the Joint Simulation System Program Manager in accordance with DoD Regulation 5000.2-R (Interim) "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisitions Programs," January 4, 2001:

a. Require Development Agents to provide complete earned value information; and

b. Construct complete life-cycle cost estimates and include requirements for which funding has not been established.

Program Office, Joint Simulation System Comments. The Program Manager stated that the Joint Simulation System security policy has been published and that the system security procedures manual and security standard operating procedures are being written. These actions were initiated in accordance with DS-2610-142-01, "DoD Intelligence Information System Security Certification and Accreditation Guide," April 2001 rather than DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997, recommended in the draft report. Funding has been requested to create a secure trusted environment for the development of the Common Component Workstation and corrective actions are ongoing to implement the recommendations addressing the Earned Value Management System and life-cycle cost estimates.

Audit Response. We considered management comments to be responsive.

Appendix A. Audit Process

Scope

We performed this audit in response to a request from the Director, Joint Staff, to evaluate the management of the Joint Simulation System. This is the second audit report on the management of the Joint Simulation System. The first report addressed specific management concerns raised by the Director, Joint Staff. This report addresses the broader topic of overall financial and program management of the development and acquisition of the Joint Simulation System.

We examined program management of JSIMS from September 2000 through April 2001 and reviewed documentation dated from November 1996 through April 2001. We visited the JSIMS PM and each of the nine DAs. We reviewed and analyzed memorandums, modifications to contracts, military interdepartmental purchase requests, accounting reports, correspondence, schedules, briefing charts, and operational and security documents.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Defense Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from September 2000 through April 2001 in accordance generally accepted Government auditing standards except that we were unable to obtain an opinion on our system of quality control. The most recent external quality control review was withdrawn on March 15, 2001, and we will undergo a new review. Accordingly, we included tests of management controls, as considered necessary.

Use of Computer-Process Data. We did not rely on computer-processed data to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within the DoD and Defense contractors. Further details are available on request.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program" August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of those controls.

Scope of the Review of the Management Control Program. For the JSIMS Program, we reviewed the plan for Internal Management and Control of Funds and management self-evaluation. Management's self-evaluation had uncovered weaknesses prior to our audit, and management had taken corrective action.

Adequacy of Management controls. We identified material management control weaknesses as defined in DoD Instruction 5010.40. System security controls were incomplete. The earned value management system controls were unreliable, and acquisition program baselines designed to assure that cost and schedule goals are met were unsatisfactory. Management actions taken during the course of the audit such as development of a Risk Management Plan combined with implementation of this report's recommendations will correct the weaknesses. We will provide a copy of this report to the senior official responsible for management controls in the office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Prior Coverage

Inspector General, DoD

Inspector General, DoD, Report No. D-2001-089, "Management Issues at the Joint Simulation System Program Office," March 30, 2001

Inspector General, DoD, Report No. 97-138, "Requirements Planning and the Impact On Readiness of Training Simulators and Devices," April 30, 1997

Appendix B. Joint Simulation System Development Agents

JSIMS will incorporate simulations across the full range of military operations. Simulations will also include geophysical, meteorological, oceanographic, and environmental factors. Those simulations will be provided by DAs from the Army, the Navy, the Air Force, and the Marine Corps for each warfare domain (land, maritime, air/space, and amphibious operations). In addition, DAs from the Intelligence Community (the Defense Intelligence Agency, the National Reconnaissance Office, and the National Security Agency) will provide intelligence related simulations. The DAs develop JSIMS software components, field and deploy the system, and provide all required software support. The integration of software is a collaborative activity in that it is led and managed by the JSIMS PM but supported by each DA partner.

Army

The Army is developing the Warfighters' Simulation System, that includes the Warfighters Simulation System Intelligence Module. The Warfighters' Simulation System will replace the Corps Battle Simulation System, the Corps Battle Simulation in Joint Training Confederation, the Combat Service Support Training Simulation System, the Brigade/Battalion Battle Simulation System, and the Tactical Simulation System. The system will provide simulation of the land warfare battle elements for JSIMS and will receive battle elements from JSIMS in areas such as joint and maritime operations, air and space, and intelligence.

Navy

The Navy portion of JSIMS is known as Maritime. Maritime is a technical effort that will provide validated battle elements that represent the maritime domain and that support the development of specialized and unique interfaces required for executing Navy and Marine Corps training evolutions. JSIMS will be used to conduct in-port shipboard combat system team training and at-sea exercises for training individual ship combat teams. Maritime is also being developed to replace legacy Navy training systems to include the Research Evaluation and Systems Analysis System and the Enhanced Naval Warfare Gaming System, that are due to lose funding by FY 2002 and FY 2004 respectively.

Air Force

The Air Force portion of JSIMS contains two components. The first component, known as the National Air and Space Model, provides Air Force aerospace simulation to JSIMS. Those simulations include battle elements such as aircraft (both fixed wing and rotary wing), weapons, electronic jammers, and generic satellite platforms. The system will provide missions, organizations, and civil environment representations. The National Air and Space Model will replace the Air Force Air Warfare Simulation training system.

The second Air Force JSIMS component is the Joint Operations Information Simulation. The component will provide the JSIMS audience with models for intelligence collection, intelligence reporting, and aspects of electronic warfare. The simulation brings a comprehensive capability to perform intelligence collection through air breathing sensors and can demonstrate electronic warfare capabilities against radars, and tactical related applications to command, control, communications, computer, and intelligence interfaces. The Joint Operations Information Simulation will not replace any Air Force legacy systems.

Marine Corps

The Marine Corps is not performing any JSIMS system development but is providing requirements and funding to the Army and Navy DAs to leverage its portion of JSIMS. The Marine Corps DA depends on the Army for land-based operation simulations and the Navy for sea-based simulations for its model development. JSIMS is a vital piece of training equipment to the Marine Corps because it will replace the Marine Air-Ground Task Force Tactical Warfare Simulation, the current Marine Corps training simulation program.

Defense Intelligence Agency

The Defense Intelligence Agency Object Oriented Model of Intelligence Operations will simulate the U.S. national intelligence cycle at joint task force, theater, and national levels. The simulation will represent the intelligence cycle systems, products, and processes performed or facilitated by the intelligence components. The system will operate in both the collateral and sensitive compartmented information enclaves of JSIMS and will provide intelligence models. The Object Oriented Model of Intelligence Operations development represents new national-level intelligence functionality that is not currently represented within the current Joint Training Confederation. There is no predecessor for this system.

National Reconnaissance Office

Developed by the National Reconnaissance Office, the National Simulation Program is the imagery intelligence component of JSIMS. It is designed to simulate the imagery intelligence cycle including collection management, resource tasking, and delivery of a message traffic textual product to respond to the initial tasking for Version Release Module 1.0. Messages will generally be at the collateral level. Future models will include a synthetic image. The National Imagery and Mapping Agency will be involved in the simulation process for imagery analysis when National Simulation Program becomes operational. The current comparable simulation system in use is the National Wargaming System managed by the National Reconnaissance Office.

National Security Agency

The National Security Agency is providing JSIMS Joint Signals Intelligence Simulation, that will provide simulations of signal intelligence capability to the warfighting community. The simulation will portray national-level signals intelligence collection, processing, analysis, and reporting functions to the warfighter. The system will produce signal intelligence products for the JSIMS training exercise in the same quantity and quality as a real operation. The simulation will interact with the intelligence portions of the other DAs to provide a comprehensive intelligence picture of the battlespace to the warfighter.

Joint Development Agent

The Joint DA is building two main functions for JSIMS; the Common Component Workstation and the joint models. The Common Component Workstation provides most of the user interfaces for JSIMS. It implements functions such as scenario generation, exercise control, unit control, and evaluation and reporting. It does not implement the exercise planning, technical control, or information system security control functions. The joint models will simulate command units at the joint task force level. Joint models operate in one of the following modes: role player without automation, role player with automation, or training audience. The Joint DA is also responsible for deployment, logistics, and training for joint locations. The Joint DA is not developing a system to replace a legacy system but is creating a new concept of functionality.

Defense Modeling and Simulation Office

The Defense Modeling and Simulation Office is the builder and advocate for High Level Architecture (HLA) throughout DoD. HLA identifies major functional elements, interfaces, and design rules pertaining as feasible to all DoD simulation applications, and provides a common framework within which specific system architectures can be defined. The Defense Modeling and Simulation Office is responsible for providing the HLA and run time infrastructure as a key component of the core of the JSIMS Program. The Defense Modeling and Simulation Office is not providing or replacing any simulations.

Appendix C. Acquisition Guidance

The Office of Management and Budget and DoD provide managers with guidance for acquiring information technology investments and safeguarding information assets.

Office of Management and Budget

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 30, 2000, implements numerous public laws and other Office of Management and Budget guidance that address acquisition of information technology investments and security of personal information. In accordance with Cohen-Clinger Act of 1996, Circular A-130 requires that:

- Cost benefit analyses be prepared for each system throughout its life cycle.

- Performance measures be implemented to provide timely information regarding the progress of an information technology program in terms of cost and capability to meet specified requirements, timeliness, and quality.

- Major information systems proceed in a timely fashion toward agreed-upon milestones in an information system life cycle.

- Chief information officers monitor and evaluate the performance of information technology investments through the capital planning investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project.

DoD Guidance

DoD Directive 5000.1. DoD Directive 5000.1, "Defense Acquisition," March 15, 1996 (subsequently revised on October 23, 2000), establishes a disciplined, life-cycle management approach for acquiring quality products. DoD Directive 5000.1 provides mandatory policies and procedures for the management of acquisition programs, including procedures to ensure program stability.

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, provides mandatory guidance for safeguarding classified information. It implements security safeguard provisions of Office of Management and Budget Circular No. A-130, and is a reference source for DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997.

DoD Instruction 5000.2. DoD Instruction 5000.2, "Operation of the Defense Acquisition System," Change 1, January 4, 2001, establishes a general approach for managing system acquisitions with best life-cycle solutions for satisfying user requirements. DoD Instruction 5000.2 requires chief information officers to confirm that mission-critical and essential information systems are developed in accordance with the Clinger-Cohen Act of 1996 before approvals are granted for contract award.

DoD Regulation 5000.2-R. DoD Regulation 5000.2-R (Interim), "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," January 4, 2001, establishes life-cycle procedures and requires earned value management on significant contracts and subcontracts within all acquisition programs.

DoD Instruction 5200.40. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997. DoD Instruction 5200.40 applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence oversees and reviews the implementation of DoD Instruction 5200.40, which establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit information technology systems that will maintain the security posture of the Defense Information Infrastructure. The key to DoD Instruction 5200.40 is the agreement between the information technology system PM, the Designated Approving Authority, the Certification Authority, and the user representative. Those managers resolve critical schedule, budget, security, functionality, and performance issues. The agreement is documented in the System Security Authorization Agreement that is used to guide and document the results of the certification and accreditation. The objective is to use the System Security Authorization Agreement to establish a binding agreement on the level of security required before the system development begins or before changes to a system are made.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller/Chief Financial Officer)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director, Investment and Acquisition

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army
Program Manager, Joint Simulation System
Program Manager, Warfighters Simulation 2000

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy
Program Manager, Joint Simulation System Maritime
Program Manager, United States Marine Corps Development Agent

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Program Manager, National Air and Space Model

Other Defense Organizations

Director, Joint Warfighting Center
Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Inspector General, National Reconnaissance Office
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organization

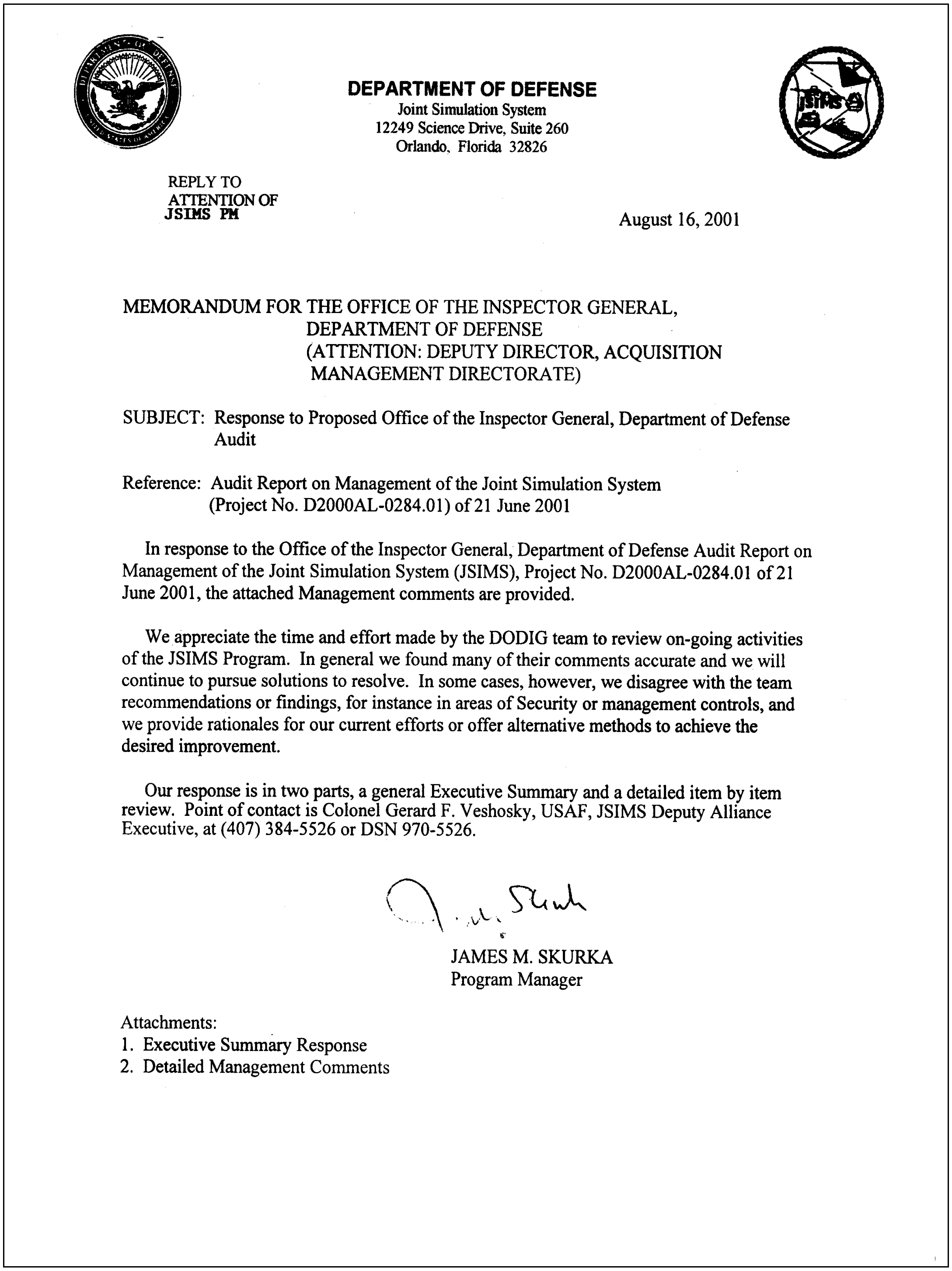
Office of Management and Budget, National Security Division

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform
House Permanent Select Committee on Intelligence

Program Office, Joint Simulation System Comments

Final Report
Reference



DEPARTMENT OF DEFENSE
Joint Simulation System
12249 Science Drive, Suite 260
Orlando, Florida 32826

REPLY TO
ATTENTION OF
JSIMS PM

August 16, 2001

MEMORANDUM FOR THE OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE
(ATTENTION: DEPUTY DIRECTOR, ACQUISITION
MANAGEMENT DIRECTORATE)

SUBJECT: Response to Proposed Office of the Inspector General, Department of Defense Audit

Reference: Audit Report on Management of the Joint Simulation System (Project No. D2000AL-0284.01) of 21 June 2001

In response to the Office of the Inspector General, Department of Defense Audit Report on Management of the Joint Simulation System (JSIMS), Project No. D2000AL-0284.01 of 21 June 2001, the attached Management comments are provided.

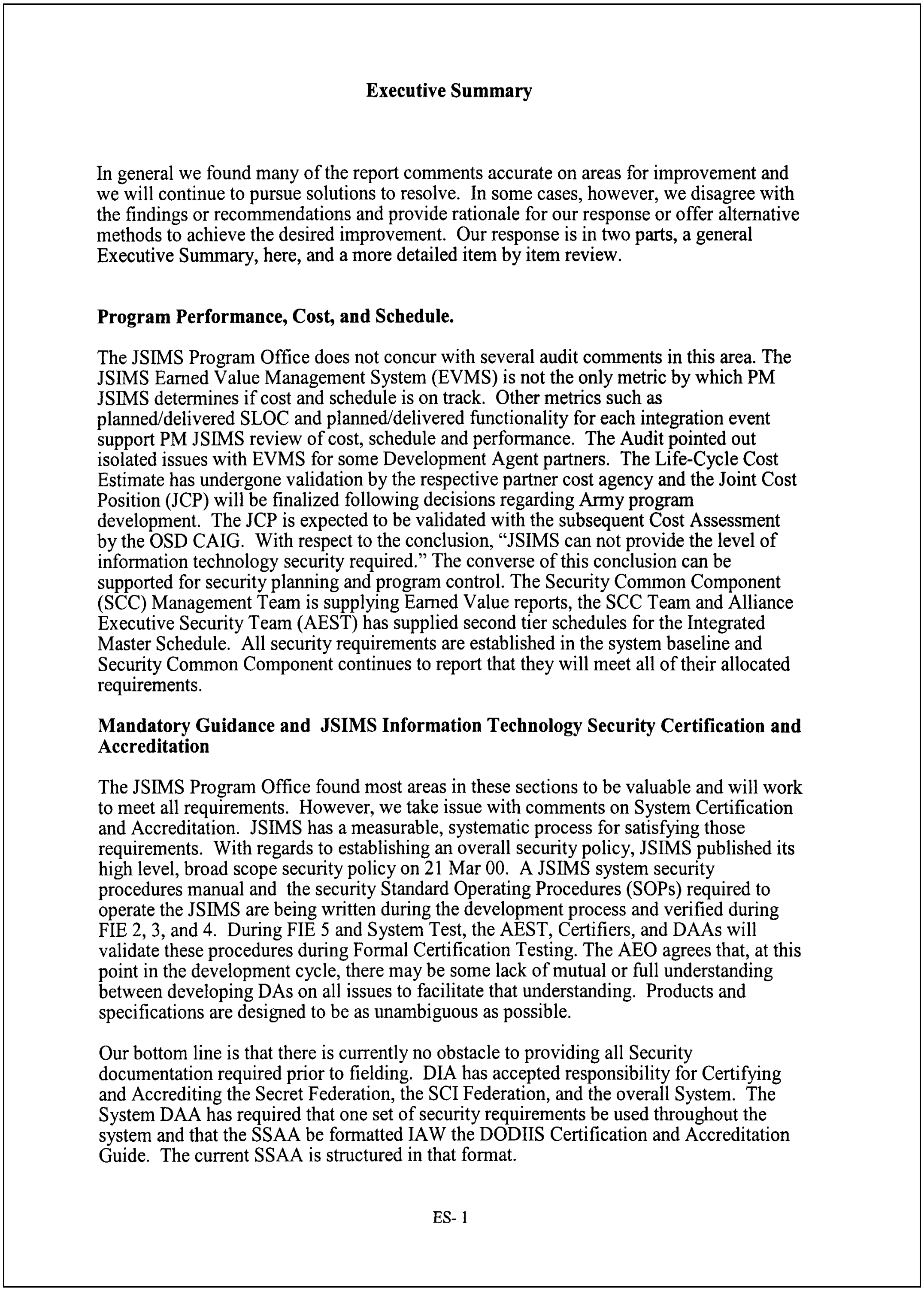
We appreciate the time and effort made by the DODIG team to review on-going activities of the JSIMS Program. In general we found many of their comments accurate and we will continue to pursue solutions to resolve. In some cases, however, we disagree with the team recommendations or findings, for instance in areas of Security or management controls, and we provide rationales for our current efforts or offer alternative methods to achieve the desired improvement.

Our response is in two parts, a general Executive Summary and a detailed item by item review. Point of contact is Colonel Gerard F. Veshosky, USAF, JSIMS Deputy Alliance Executive, at (407) 384-5526 or DSN 970-5526.

JAMES M. SKURKA
Program Manager

Attachments:
1. Executive Summary Response
2. Detailed Management Comments

Final Report Reference



Executive Summary

In general we found many of the report comments accurate on areas for improvement and we will continue to pursue solutions to resolve. In some cases, however, we disagree with the findings or recommendations and provide rationale for our response or offer alternative methods to achieve the desired improvement. Our response is in two parts, a general Executive Summary, here, and a more detailed item by item review.

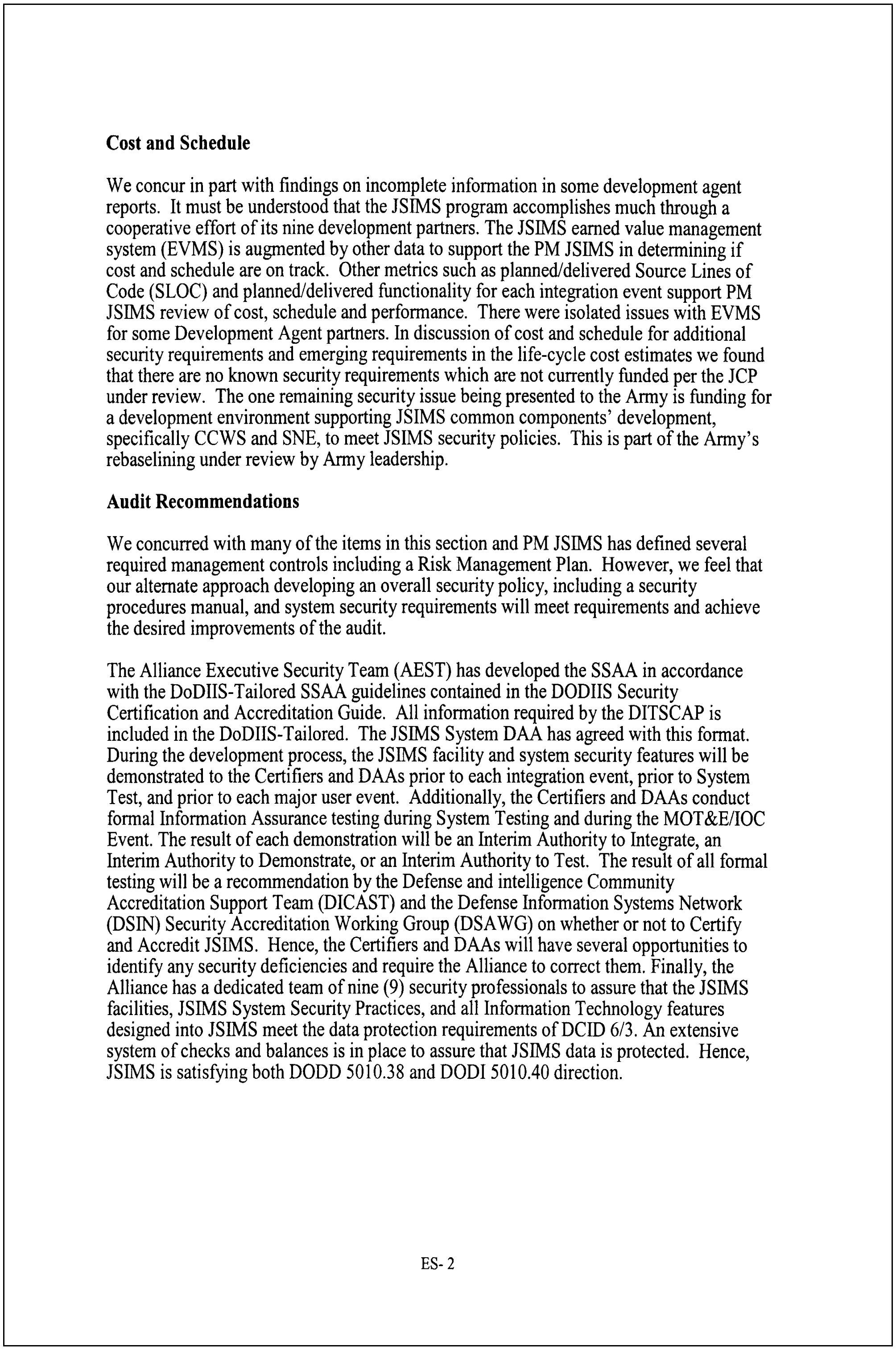
Program Performance, Cost, and Schedule.

The JSIMS Program Office does not concur with several audit comments in this area. The JSIMS Earned Value Management System (EVMS) is not the only metric by which PM JSIMS determines if cost and schedule is on track. Other metrics such as planned/delivered SLOC and planned/delivered functionality for each integration event support PM JSIMS review of cost, schedule and performance. The Audit pointed out isolated issues with EVMS for some Development Agent partners. The Life-Cycle Cost Estimate has undergone validation by the respective partner cost agency and the Joint Cost Position (JCP) will be finalized following decisions regarding Army program development. The JCP is expected to be validated with the subsequent Cost Assessment by the OSD CAIG. With respect to the conclusion, “JSIMS can not provide the level of information technology security required.” The converse of this conclusion can be supported for security planning and program control. The Security Common Component (SCC) Management Team is supplying Earned Value reports, the SCC Team and Alliance Executive Security Team (AEST) has supplied second tier schedules for the Integrated Master Schedule. All security requirements are established in the system baseline and Security Common Component continues to report that they will meet all of their allocated requirements.

Mandatory Guidance and JSIMS Information Technology Security Certification and Accreditation

The JSIMS Program Office found most areas in these sections to be valuable and will work to meet all requirements. However, we take issue with comments on System Certification and Accreditation. JSIMS has a measurable, systematic process for satisfying those requirements. With regards to establishing an overall security policy, JSIMS published its high level, broad scope security policy on 21 Mar 00. A JSIMS system security procedures manual and the security Standard Operating Procedures (SOPs) required to operate the JSIMS are being written during the development process and verified during FIE 2, 3, and 4. During FIE 5 and System Test, the AEST, Certifiers, and DAAs will validate these procedures during Formal Certification Testing. The AEO agrees that, at this point in the development cycle, there may be some lack of mutual or full understanding between developing DAs on all issues to facilitate that understanding. Products and specifications are designed to be as unambiguous as possible.

Our bottom line is that there is currently no obstacle to providing all Security documentation required prior to fielding. DIA has accepted responsibility for Certifying and Accrediting the Secret Federation, the SCI Federation, and the overall System. The System DAA has required that one set of security requirements be used throughout the system and that the SSAA be formatted IAW the DODIIS Certification and Accreditation Guide. The current SSAA is structured in that format.



Cost and Schedule

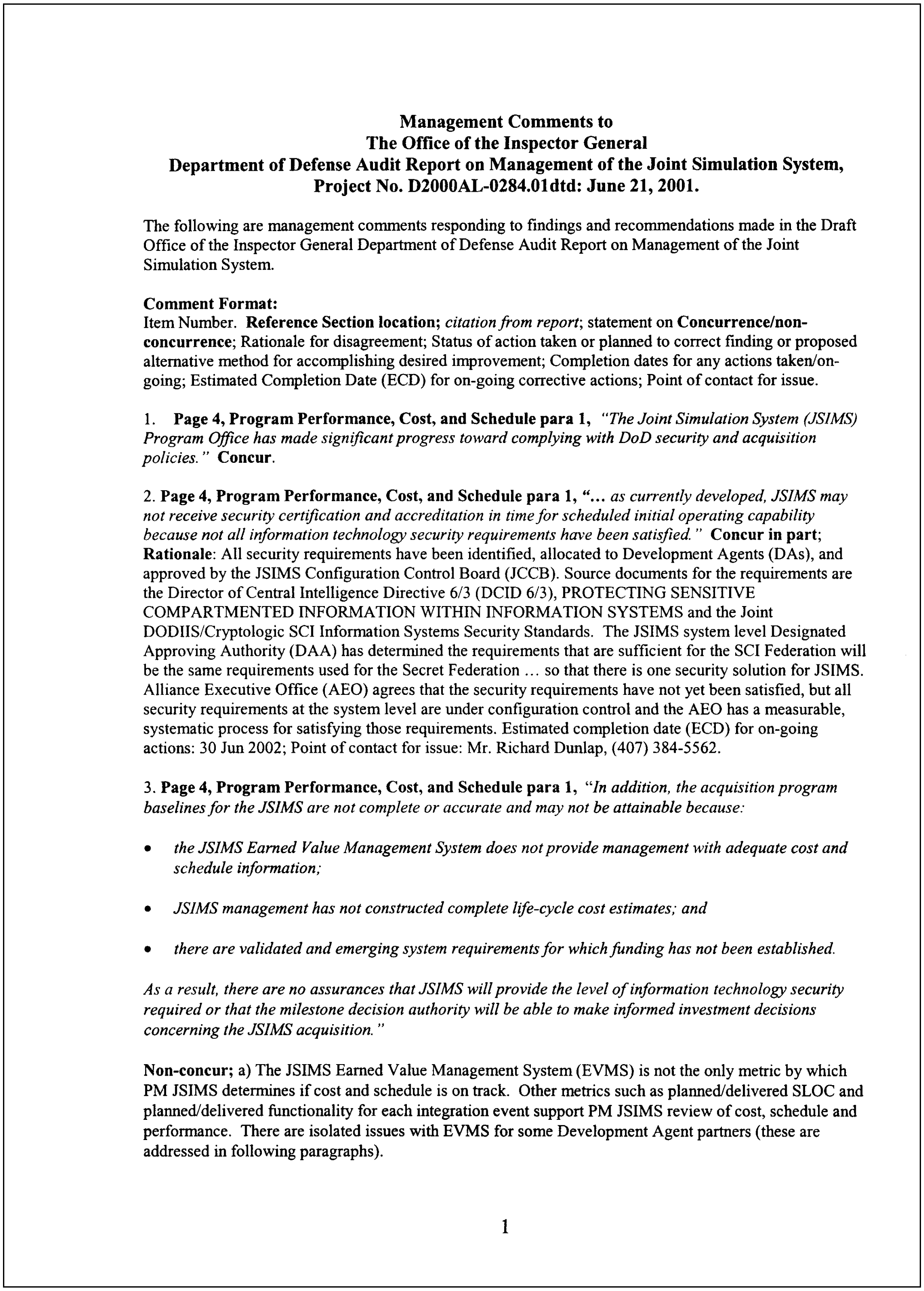
We concur in part with findings on incomplete information in some development agent reports. It must be understood that the JSIMS program accomplishes much through a cooperative effort of its nine development partners. The JSIMS earned value management system (EVMS) is augmented by other data to support the PM JSIMS in determining if cost and schedule are on track. Other metrics such as planned/delivered Source Lines of Code (SLOC) and planned/delivered functionality for each integration event support PM JSIMS review of cost, schedule and performance. There were isolated issues with EVMS for some Development Agent partners. In discussion of cost and schedule for additional security requirements and emerging requirements in the life-cycle cost estimates we found that there are no known security requirements which are not currently funded per the JCP under review. The one remaining security issue being presented to the Army is funding for a development environment supporting JSIMS common components' development, specifically CCWS and SNE, to meet JSIMS security policies. This is part of the Army's rebaselining under review by Army leadership.

Audit Recommendations

We concurred with many of the items in this section and PM JSIMS has defined several required management controls including a Risk Management Plan. However, we feel that our alternate approach developing an overall security policy, including a security procedures manual, and system security requirements will meet requirements and achieve the desired improvements of the audit.

The Alliance Executive Security Team (AEST) has developed the SSAA in accordance with the DoDIIS-Tailored SSAA guidelines contained in the DODIIS Security Certification and Accreditation Guide. All information required by the DITSCAP is included in the DoDIIS-Tailored. The JSIMS System DAA has agreed with this format. During the development process, the JSIMS facility and system security features will be demonstrated to the Certifiers and DAAs prior to each integration event, prior to System Test, and prior to each major user event. Additionally, the Certifiers and DAAs conduct formal Information Assurance testing during System Testing and during the MOT&E/IOC Event. The result of each demonstration will be an Interim Authority to Integrate, an Interim Authority to Demonstrate, or an Interim Authority to Test. The result of all formal testing will be a recommendation by the Defense and intelligence Community Accreditation Support Team (DICAST) and the Defense Information Systems Network (DSIN) Security Accreditation Working Group (DSAWG) on whether or not to Certify and Accredit JSIMS. Hence, the Certifiers and DAAs will have several opportunities to identify any security deficiencies and require the Alliance to correct them. Finally, the Alliance has a dedicated team of nine (9) security professionals to assure that the JSIMS facilities, JSIMS System Security Practices, and all Information Technology features designed into JSIMS meet the data protection requirements of DCID 6/3. An extensive system of checks and balances is in place to assure that JSIMS data is protected. Hence, JSIMS is satisfying both DODD 5010.38 and DODI 5010.40 direction.

Final Report Reference



Management Comments to
The Office of the Inspector General
Department of Defense Audit Report on Management of the Joint Simulation System,
Project No. D2000AL-0284.01dtd: June 21, 2001.

The following are management comments responding to findings and recommendations made in the Draft Office of the Inspector General Department of Defense Audit Report on Management of the Joint Simulation System.

Comment Format:
Item Number. **Reference Section location;** *citation from report*; statement on **Concurrence/non-concurrence**; Rationale for disagreement; Status of action taken or planned to correct finding or proposed alternative method for accomplishing desired improvement; Completion dates for any actions taken/on-going; Estimated Completion Date (ECD) for on-going corrective actions; Point of contact for issue.

Pg 4

1. **Page 4, Program Performance, Cost, and Schedule para 1,** *"The Joint Simulation System (JSIMS) Program Office has made significant progress toward complying with DoD security and acquisition policies."* **Concur**.

Pg 4

2. **Page 4, Program Performance, Cost, and Schedule para 1, "**... *as currently developed, JSIMS may not receive security certification and accreditation in time for scheduled initial operating capability because not all information technology security requirements have been satisfied."* **Concur in part**; **Rationale**: All security requirements have been identified, allocated to Development Agents (DAs), and approved by the JSIMS Configuration Control Board (JCCB). Source documents for the requirements are the Director of Central Intelligence Directive 6/3 (DCID 6/3), PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS and the Joint DODIIS/Cryptologic SCI Information Systems Security Standards. The JSIMS system level Designated Approving Authority (DAA) has determined the requirements that are sufficient for the SCI Federation will be the same requirements used for the Secret Federation ... so that there is one security solution for JSIMS. Alliance Executive Office (AEO) agrees that the security requirements have not yet been satisfied, but all security requirements at the system level are under configuration control and the AEO has a measurable, systematic process for satisfying those requirements. Estimated completion date (ECD) for on-going actions: 30 Jun 2002; Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 4

3. **Page 4, Program Performance, Cost, and Schedule para 1,** *"In addition, the acquisition program baselines for the JSIMS are not complete or accurate and may not be attainable because:*

- *the JSIMS Earned Value Management System does not provide management with adequate cost and schedule information;*
- *JSIMS management has not constructed complete life-cycle cost estimates; and*
- *there are validated and emerging system requirements for which funding has not been established.*

As a result, there are no assurances that JSIMS will provide the level of information technology security required or that the milestone decision authority will be able to make informed investment decisions concerning the JSIMS acquisition."

Non-concur; a) The JSIMS Earned Value Management System (EVMS) is not the only metric by which PM JSIMS determines if cost and schedule is on track. Other metrics such as planned/delivered SLOC and planned/delivered functionality for each integration event support PM JSIMS review of cost, schedule and performance. There are isolated issues with EVMS for some Development Agent partners (these are addressed in following paragraphs).

b) The Life-Cycle Cost Estimate has undergone validation by the respective partner cost agency and the Joint Cost Position (JCP) will be finalized following decisions regarding Army program development. The JCP is expected to be validated with the subsequent Cost Assessment by the OSD CAIG.

c) The JSIMS users consisting of the Services, Joint Commands and Intelligence Agencies have the ability to submit and/or update requirements for JSIMS. All requirements are reviewed and prioritized by the JSIMS Requirements Control Board (JRCB) for each Version Release. Requirements are viewed as to the threshold required and the objective for each funding within the funding constraints of all program partners. Emerging requirements may or may not take precedence over existing ones. Point of contact for issue: G.S. Crabtree, 407-384-5563

With respect to (WRT) the conclusion, "JSIMS can not provide the level of information technology security required." **Non-Concur**; The converse of this conclusion can be supported for security planning and program control. The Security Common Component (SCC) Management Team is supplying Earned Value reports, the SCC Team and Alliance Executive Security Team (AEST) has supplied second tier schedules for the Integrated Master Schedule. The AEST provided life-cycle cost estimates to the CARD (and budgeted for those costs), and all system level security requirements have been funded, derived, sequenced, and approved by the JCCB. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

4. **Page 4, Mandatory Guidance para 2,** "*When the audit began in September 2000, required Acquisition Category ID program documents such as the Acquisition Strategy, the Test and Evaluation Management Plan, and the Risk Management Plan did not exist.*" **Concur.** Pg 4

5. **Page 4, Mandatory Guidance para 2,** "*Further, the JSIMS program was not in compliance with the information technology acquisition requirements of the Clinger-Cohen Act, which requires economic analysis, performance measures, business process reengineering, and an information assurance strategy.*" **Concur in part;** As of September 2000. Since that time JSIMS has registered as an Information Technology Program and developed an information assurance strategy. Performance measures have been established as part of PM JSIMS review. Point of contact for issue: G.S. Crabtree, 407-384-5563. Pg 4

6. **Page 4, Mandatory Guidance para 2,** "*Specifically, the JSIMS PM had no documentation regarding JSIMS compliance with the Clinger-Cohen Act.*[1]" **Concur in part**; As of September 2000. Since that time JSIMS has registered with the Army as a Mission Critical Information Technology program. JSIMS continues to develop required program documentation including that required for CCA compliance. ECD is 15 Feb 2002. Point of contact for issue: G.S. Crabtree, 407-384-5563. Pg 4

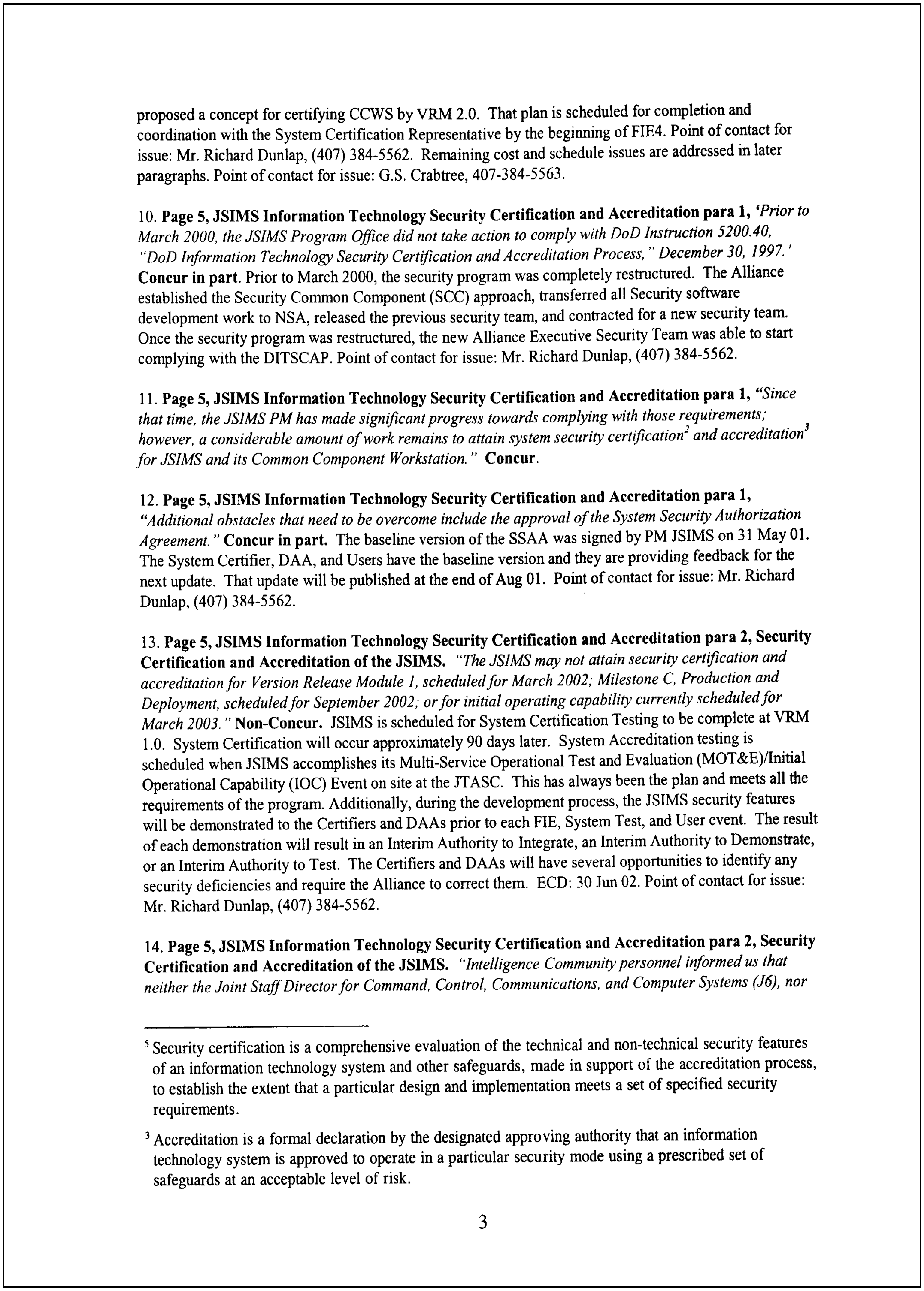
7. **Page 5, Mandatory Guidance para 2,** "*During the course of the audit, the new JSIMS management team worked diligently to generate the documents needed to comply with DoD policy and congressional direction.*" **Concur.** Pg 5

8. **Page 5, Mandatory Guidance para 2,** "*Although some of these documents are not yet finalized, the JSIMS PM has taken seriously his obligation to adhere to DoD policy and is making significant progress towards attaining compliance, thereby reducing our concerns in those areas.*" **Concur.** Pg 5

9. **Page 5, Mandatory Guidance para 2,** "*However, the JSIMS and its Common Component Workstation will have a difficult time obtaining system security certification and accreditation. Further, several factors may impact the attainability of JSIMS cost and schedule objectives.*" **Concur in part.** CCWS will not be certified for use in the SCI environment for VRM 1.0. This issue was vetted through the Alliance Issue Process, and the Users agreed to a satisfactory workaround for VRM 1.0. Additionally, the AEST has Pg 5

[1] The Act governs the acquisition of information technology, which requires Chief Information Officer monitoring of system acquisition and the establishment of performance measures regarding progress towards meeting program objectives.

Final Report Reference



proposed a concept for certifying CCWS by VRM 2.0. That plan is scheduled for completion and coordination with the System Certification Representative by the beginning of FIE4. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562. Remaining cost and schedule issues are addressed in later paragraphs. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 5

10. **Page 5, JSIMS Information Technology Security Certification and Accreditation para 1,** *'Prior to March 2000, the JSIMS Program Office did not take action to comply with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997.'* **Concur in part**. Prior to March 2000, the security program was completely restructured. The Alliance established the Security Common Component (SCC) approach, transferred all Security software development work to NSA, released the previous security team, and contracted for a new security team. Once the security program was restructured, the new Alliance Executive Security Team was able to start complying with the DITSCAP. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 5

11. **Page 5, JSIMS Information Technology Security Certification and Accreditation para 1,** *"Since that time, the JSIMS PM has made significant progress towards complying with those requirements; however, a considerable amount of work remains to attain system security certification[2] and accreditation[3] for JSIMS and its Common Component Workstation."* **Concur**.

Pg 5

12. **Page 5, JSIMS Information Technology Security Certification and Accreditation para 1,** *"Additional obstacles that need to be overcome include the approval of the System Security Authorization Agreement."* **Concur in part.** The baseline version of the SSAA was signed by PM JSIMS on 31 May 01. The System Certifier, DAA, and Users have the baseline version and they are providing feedback for the next update. That update will be published at the end of Aug 01. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 5

13. **Page 5, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS.** *"The JSIMS may not attain security certification and accreditation for Version Release Module 1, scheduled for March 2002; Milestone C, Production and Deployment, scheduled for September 2002; or for initial operating capability currently scheduled for March 2003."* **Non-Concur.** JSIMS is scheduled for System Certification Testing to be complete at VRM 1.0. System Certification will occur approximately 90 days later. System Accreditation testing is scheduled when JSIMS accomplishes its Multi-Service Operational Test and Evaluation (MOT&E)/Initial Operational Capability (IOC) Event on site at the JTASC. This has always been the plan and meets all the requirements of the program. Additionally, during the development process, the JSIMS security features will be demonstrated to the Certifiers and DAAs prior to each FIE, System Test, and User event. The result of each demonstration will result in an Interim Authority to Integrate, an Interim Authority to Demonstrate, or an Interim Authority to Test. The Certifiers and DAAs will have several opportunities to identify any security deficiencies and require the Alliance to correct them. ECD: 30 Jun 02. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

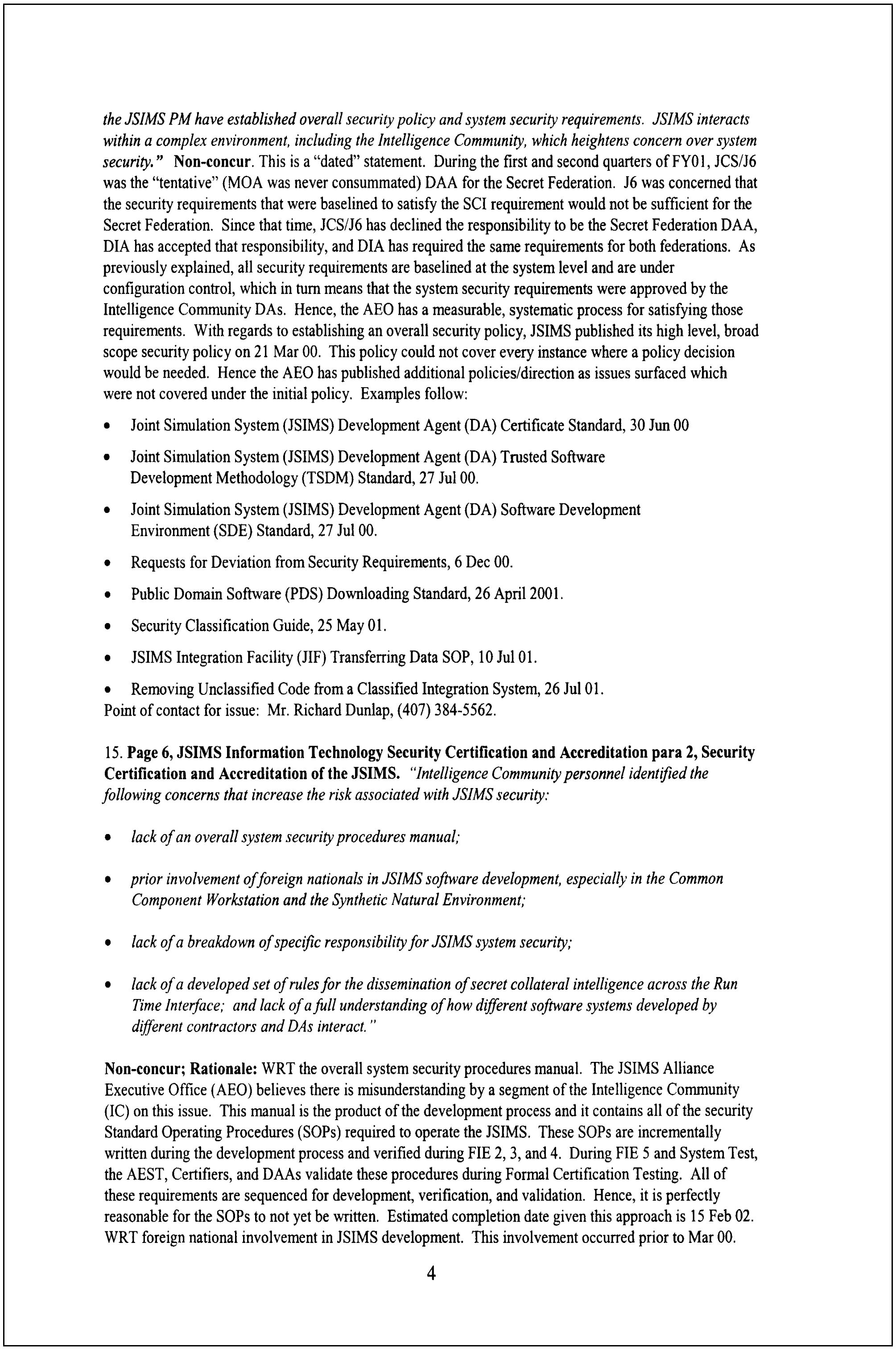
Revised Pg 5

14. **Page 5, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS.** *"Intelligence Community personnel informed us that neither the Joint Staff Director for Command, Control, Communications, and Computer Systems (J6), nor*

[5] Security certification is a comprehensive evaluation of the technical and non-technical security features of an information technology system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

[3] Accreditation is a formal declaration by the designated approving authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Final Report Reference



the JSIMS PM have established overall security policy and system security requirements. JSIMS interacts within a complex environment, including the Intelligence Community, which heightens concern over system security." **Non-concur**. This is a "dated" statement. During the first and second quarters of FY01, JCS/J6 was the "tentative" (MOA was never consummated) DAA for the Secret Federation. J6 was concerned that the security requirements that were baselined to satisfy the SCI requirement would not be sufficient for the Secret Federation. Since that time, JCS/J6 has declined the responsibility to be the Secret Federation DAA, DIA has accepted that responsibility, and DIA has required the same requirements for both federations. As previously explained, all security requirements are baselined at the system level and are under configuration control, which in turn means that the system security requirements were approved by the Intelligence Community DAs. Hence, the AEO has a measurable, systematic process for satisfying those requirements. With regards to establishing an overall security policy, JSIMS published its high level, broad scope security policy on 21 Mar 00. This policy could not cover every instance where a policy decision would be needed. Hence the AEO has published additional policies/direction as issues surfaced which were not covered under the initial policy. Examples follow:

- Joint Simulation System (JSIMS) Development Agent (DA) Certificate Standard, 30 Jun 00
- Joint Simulation System (JSIMS) Development Agent (DA) Trusted Software Development Methodology (TSDM) Standard, 27 Jul 00.
- Joint Simulation System (JSIMS) Development Agent (DA) Software Development Environment (SDE) Standard, 27 Jul 00.
- Requests for Deviation from Security Requirements, 6 Dec 00.
- Public Domain Software (PDS) Downloading Standard, 26 April 2001.
- Security Classification Guide, 25 May 01.
- JSIMS Integration Facility (JIF) Transferring Data SOP, 10 Jul 01.
- Removing Unclassified Code from a Classified Integration System, 26 Jul 01.

Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

15. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS.** *"Intelligence Community personnel identified the following concerns that increase the risk associated with JSIMS security:* Pg 5

- *lack of an overall system security procedures manual;*
- *prior involvement of foreign nationals in JSIMS software development, especially in the Common Component Workstation and the Synthetic Natural Environment;*
- *lack of a breakdown of specific responsibility for JSIMS system security;*
- *lack of a developed set of rules for the dissemination of secret collateral intelligence across the Run Time Interface; and lack of a full understanding of how different software systems developed by different contractors and DAs interact."*

Non-concur; Rationale: WRT the overall system security procedures manual. The JSIMS Alliance Executive Office (AEO) believes there is misunderstanding by a segment of the Intelligence Community (IC) on this issue. This manual is the product of the development process and it contains all of the security Standard Operating Procedures (SOPs) required to operate the JSIMS. These SOPs are incrementally written during the development process and verified during FIE 2, 3, and 4. During FIE 5 and System Test, the AEST, Certifiers, and DAAs validate these procedures during Formal Certification Testing. All of these requirements are sequenced for development, verification, and validation. Hence, it is perfectly reasonable for the SOPs to not yet be written. Estimated completion date given this approach is 15 Feb 02. WRT foreign national involvement in JSIMS development. This involvement occurred prior to Mar 00.

Final Report
Reference

During the period of Mar 00 to Jun 00, the AEO briefed the DAs that a secure development environment would be needed for JSIMS to be accredited. Between Jun 00 and Jul 00, the AEO published standards that expressly precluded the use of foreign nationals and required DAs to document the pedigree of the software turned over for integration. The AEO has assurances from all DAs that foreign nationals are no longer building software targeted for use on JSIMS. WRT lack of specific responsibility for JSIMS system security., On 1 Dec 00, the AEST submitted System Problem Report (SPR) 22 to the JCCB for approval. Contained in that SPR were all of the System Level Security Requirements and their specific allocation to individual DAs for development, integration, and support. Hence the AEO believes there is a misunderstanding on the status of the security requirements on part of the IC. WRT lack of a developed set of rules for dissemination of Secret Collateral data across the RTI. The AEO agrees that there is a need for these rules and furthermore, the set of rules needs to be the same for both the Secret and SCI Federations. Those rules are included in the Federation Object Model (FOM) specification. The FOM specification is updated for each FIE as needed to support the next event. The part of the FOM specification that addresses the passing of classified information across the RTI is currently being developed for implementation during FI4. Hence, it is a requirement yet to be filled, but sequenced for development. WRT the lack of a full understanding of how different software systems developed by different contractors and DAs interact. The AEO agrees that, at this point in the development cycle, there is a lack of mutual or full understanding between developing DAs on all issues. Products and specifications are designed to be as unambiguous as possible. Mutual understanding will grow as integration progresses. ECD for on-going actions: 30 Jun 02. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 6

16. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS**, *"The decentralized management of the JSIMS, and the perception by the JSIMS PM and DAs that JSIMS is just a training system, resulted in security receiving little attention prior to the December 1999 reorganization directed by the Under Secretary of Defense for Acquisition, Technology, and Logistics".* **Concur in part.** The System Level Security Requirements for JSIMS are now driven by the classification of the internal data, the classification level of interconnected C4I systems, and the use of the training system. Those requirements have been formally approved by the JCCB and formally allocated to all DAs. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

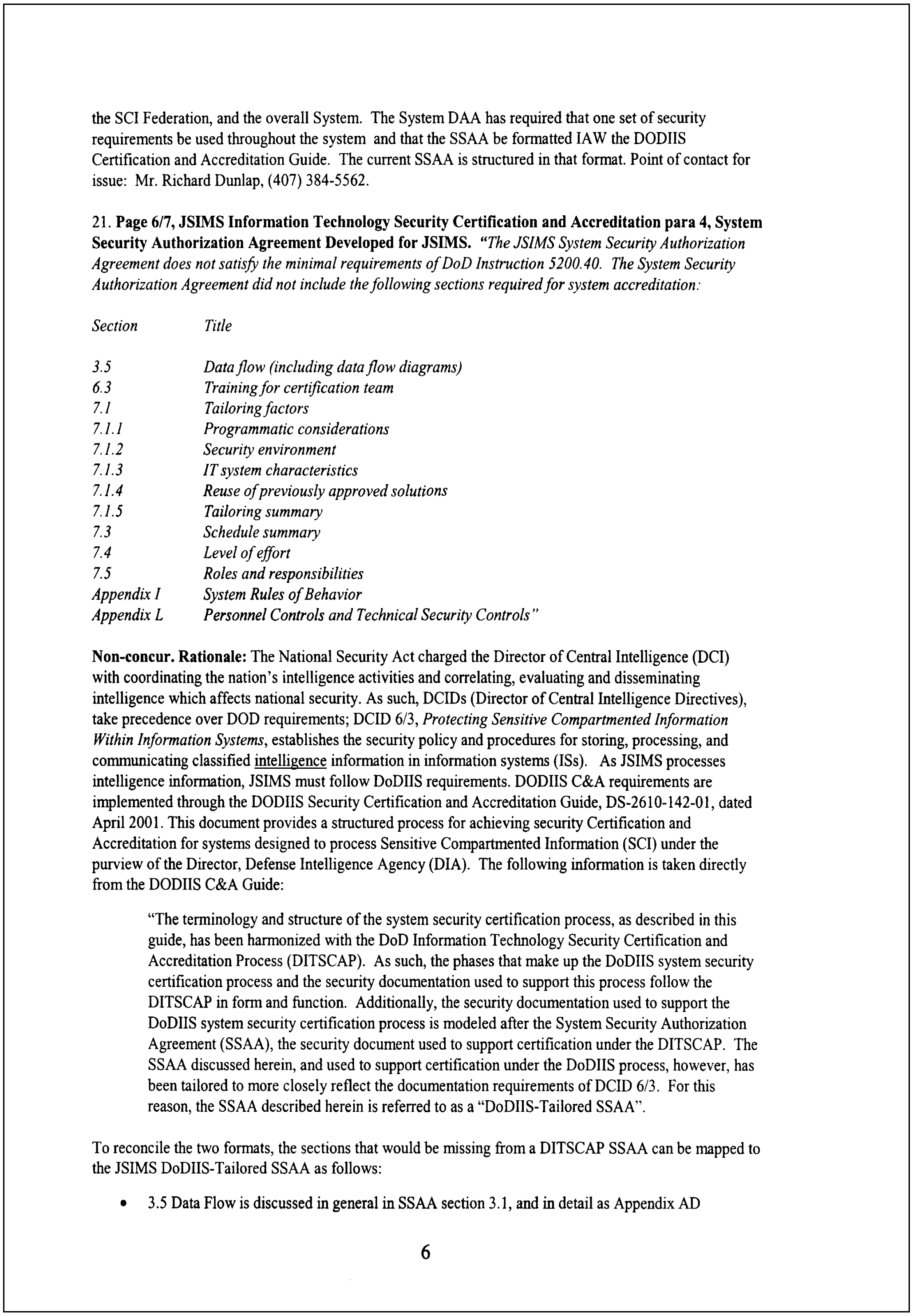
Pg 6

17. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS,** *"Beginning in March 2000, the JSIMS PM made system security certification and accreditation a major item of concern."* **Concur.** 18. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 2, Security Certification and Accreditation of the JSIMS,** *"However, JSIMS will have a difficult time achieving certification and accreditation by March 2003."* **Concur in part.** Given the sheer complexity of the JSIMS design, the need to integrate multiple independent developers, the requirement to satisfy security requirements across multiple security domains, the diversity of real world databases used and C4I systems connected, and the short time to accomplish all of this certifying and accrediting JSIMS will be a major challenge. However, based on current planning, there is currently no obstacle to achieving this by March 2003. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 6

19. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 4, System Security Authorization Agreement Developed for JSIMS.** **"***The JSIMS PM has made enormous progress in developing the System Security Authorization Agreement since our initial visit."* **Concur.** 20. **Page 6, JSIMS Information Technology Security Certification and Accreditation para 4, System Security Authorization Agreement Developed for JSIMS.** **"...***we found that the current format used to construct the System Security Authorization Agreement was not complete enough to obtain accreditation and certification."* **Non-Concur.** At the time this statement was written, the Alliance was negotiating with JCS/J6 to accredit the Secret Federation. JCS/J6 uses the DITSCAP format for accrediting Secret systems. The SSAA was formatted IAW the DODIIS Certification and Accreditation Guide, which is the format used by the System and SCI Federation DAA. Since that time, JCS/J6 has declined to be the Secret Federation DAA, and DIA has accepted responsibility for Certifying and Accrediting the Secret Federation,

Final Report
Reference



the SCI Federation, and the overall System. The System DAA has required that one set of security requirements be used throughout the system and that the SSAA be formatted IAW the DODIIS Certification and Accreditation Guide. The current SSAA is structured in that format. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Revised
Pg 6

21. **Page 6/7, JSIMS Information Technology Security Certification and Accreditation para 4, System Security Authorization Agreement Developed for JSIMS.** *"The JSIMS System Security Authorization Agreement does not satisfy the minimal requirements of DoD Instruction 5200.40. The System Security Authorization Agreement did not include the following sections required for system accreditation:*

Section	*Title*
3.5	*Data flow (including data flow diagrams)*
6.3	*Training for certification team*
7.1	*Tailoring factors*
7.1.1	*Programmatic considerations*
7.1.2	*Security environment*
7.1.3	*IT system characteristics*
7.1.4	*Reuse of previously approved solutions*
7.1.5	*Tailoring summary*
7.3	*Schedule summary*
7.4	*Level of effort*
7.5	*Roles and responsibilities*
Appendix I	*System Rules of Behavior*
Appendix L	*Personnel Controls and Technical Security Controls"*

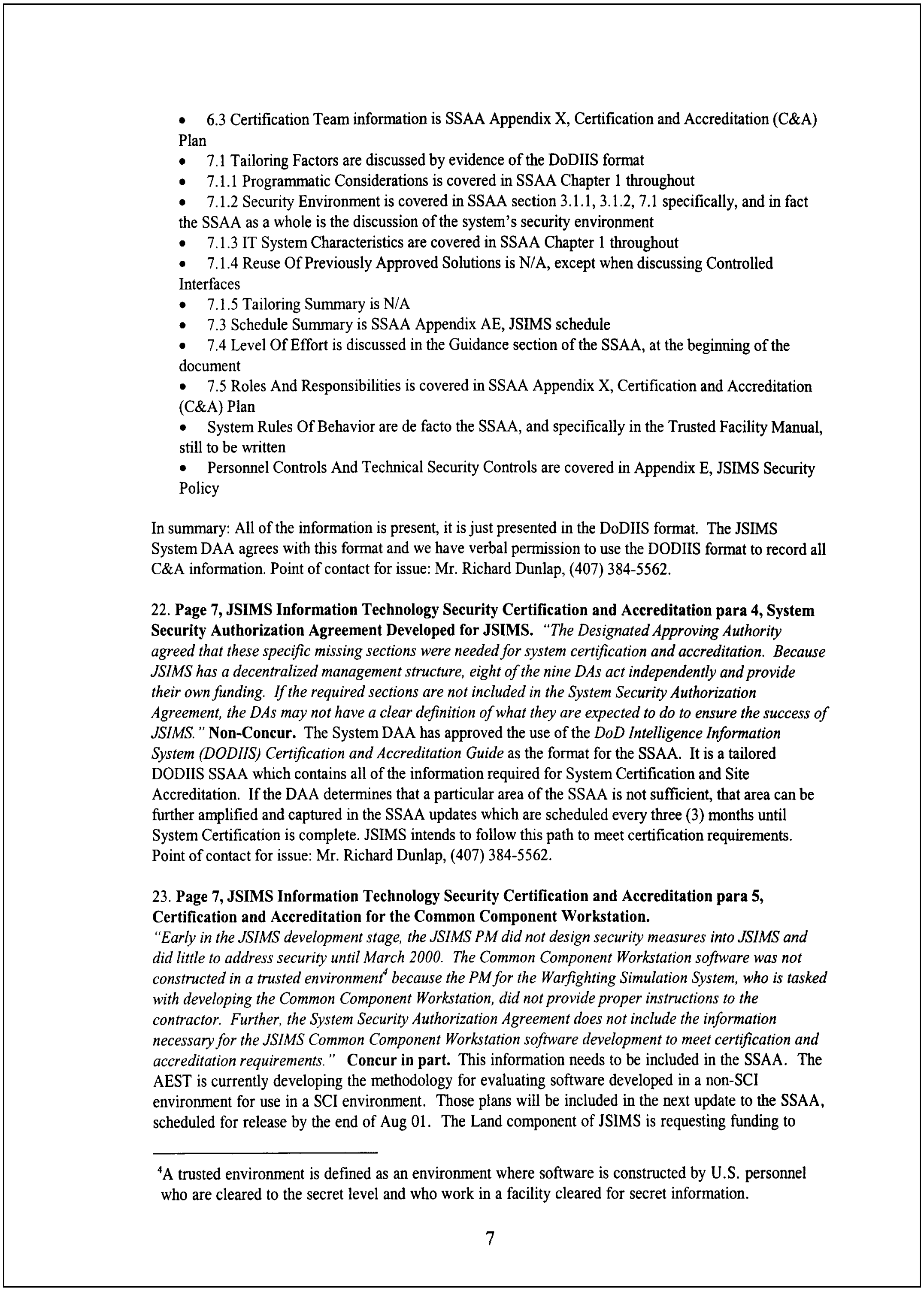
Non-concur. Rationale: The National Security Act charged the Director of Central Intelligence (DCI) with coordinating the nation's intelligence activities and correlating, evaluating and disseminating intelligence which affects national security. As such, DCIDs (Director of Central Intelligence Directives), take precedence over DOD requirements; DCID 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems (ISs). As JSIMS processes intelligence information, JSIMS must follow DoDIIS requirements. DODIIS C&A requirements are implemented through the DODIIS Security Certification and Accreditation Guide, DS-2610-142-01, dated April 2001. This document provides a structured process for achieving security Certification and Accreditation for systems designed to process Sensitive Compartmented Information (SCI) under the purview of the Director, Defense Intelligence Agency (DIA). The following information is taken directly from the DODIIS C&A Guide:

> "The terminology and structure of the system security certification process, as described in this guide, has been harmonized with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). As such, the phases that make up the DoDIIS system security certification process and the security documentation used to support this process follow the DITSCAP in form and function. Additionally, the security documentation used to support the DoDIIS system security certification process is modeled after the System Security Authorization Agreement (SSAA), the security document used to support certification under the DITSCAP. The SSAA discussed herein, and used to support certification under the DoDIIS process, however, has been tailored to more closely reflect the documentation requirements of DCID 6/3. For this reason, the SSAA described herein is referred to as a "DoDIIS-Tailored SSAA".

To reconcile the two formats, the sections that would be missing from a DITSCAP SSAA can be mapped to the JSIMS DoDIIS-Tailored SSAA as follows:

- 3.5 Data Flow is discussed in general in SSAA section 3.1, and in detail as Appendix AD

Final Report Reference



- 6.3 Certification Team information is SSAA Appendix X, Certification and Accreditation (C&A) Plan
- 7.1 Tailoring Factors are discussed by evidence of the DoDIIS format
- 7.1.1 Programmatic Considerations is covered in SSAA Chapter 1 throughout
- 7.1.2 Security Environment is covered in SSAA section 3.1.1, 3.1.2, 7.1 specifically, and in fact the SSAA as a whole is the discussion of the system's security environment
- 7.1.3 IT System Characteristics are covered in SSAA Chapter 1 throughout
- 7.1.4 Reuse Of Previously Approved Solutions is N/A, except when discussing Controlled Interfaces
- 7.1.5 Tailoring Summary is N/A
- 7.3 Schedule Summary is SSAA Appendix AE, JSIMS schedule
- 7.4 Level Of Effort is discussed in the Guidance section of the SSAA, at the beginning of the document
- 7.5 Roles And Responsibilities is covered in SSAA Appendix X, Certification and Accreditation (C&A) Plan
- System Rules Of Behavior are de facto the SSAA, and specifically in the Trusted Facility Manual, still to be written
- Personnel Controls And Technical Security Controls are covered in Appendix E, JSIMS Security Policy

In summary: All of the information is present, it is just presented in the DoDIIS format. The JSIMS System DAA agrees with this format and we have verbal permission to use the DODIIS format to record all C&A information. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Revised Pg 6

22. **Page 7, JSIMS Information Technology Security Certification and Accreditation para 4, System Security Authorization Agreement Developed for JSIMS.** *"The Designated Approving Authority agreed that these specific missing sections were needed for system certification and accreditation. Because JSIMS has a decentralized management structure, eight of the nine DAs act independently and provide their own funding. If the required sections are not included in the System Security Authorization Agreement, the DAs may not have a clear definition of what they are expected to do to ensure the success of JSIMS."* **Non-Concur.** The System DAA has approved the use of the *DoD Intelligence Information System (DODIIS) Certification and Accreditation Guide* as the format for the SSAA. It is a tailored DODIIS SSAA which contains all of the information required for System Certification and Site Accreditation. If the DAA determines that a particular area of the SSAA is not sufficient, that area can be further amplified and captured in the SSAA updates which are scheduled every three (3) months until System Certification is complete. JSIMS intends to follow this path to meet certification requirements. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 7

23. **Page 7, JSIMS Information Technology Security Certification and Accreditation para 5, Certification and Accreditation for the Common Component Workstation.** *"Early in the JSIMS development stage, the JSIMS PM did not design security measures into JSIMS and did little to address security until March 2000. The Common Component Workstation software was not constructed in a trusted environment[4] because the PM for the Warfighting Simulation System, who is tasked with developing the Common Component Workstation, did not provide proper instructions to the contractor. Further, the System Security Authorization Agreement does not include the information necessary for the JSIMS Common Component Workstation software development to meet certification and accreditation requirements."* **Concur in part.** This information needs to be included in the SSAA. The AEST is currently developing the methodology for evaluating software developed in a non-SCI environment for use in a SCI environment. Those plans will be included in the next update to the SSAA, scheduled for release by the end of Aug 01. The Land component of JSIMS is requesting funding to

[4] A trusted environment is defined as an environment where software is constructed by U.S. personnel who are cleared to the secret level and who work in a facility cleared for secret information.

Final Report Reference

correct the CCWS development environment. Estimated completion date for correction of CCWS development environment is March 2002; Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 7 24. **Page 7, JSIMS Information Technology Security Certification and Accreditation para 5, Certification and Accreditation for the Common Component Workstation.** *"The JSIMS PM will have difficulty addressing these security issues prior to the established Initial Operating Capability date."* **Concur.** The Plan for Certifying CCWS will be available at the start of FIE4, and be included in the end of Nov SSAA update. The User has provisionally agreed to this concept pending approval of the CCWS Certification Plan. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

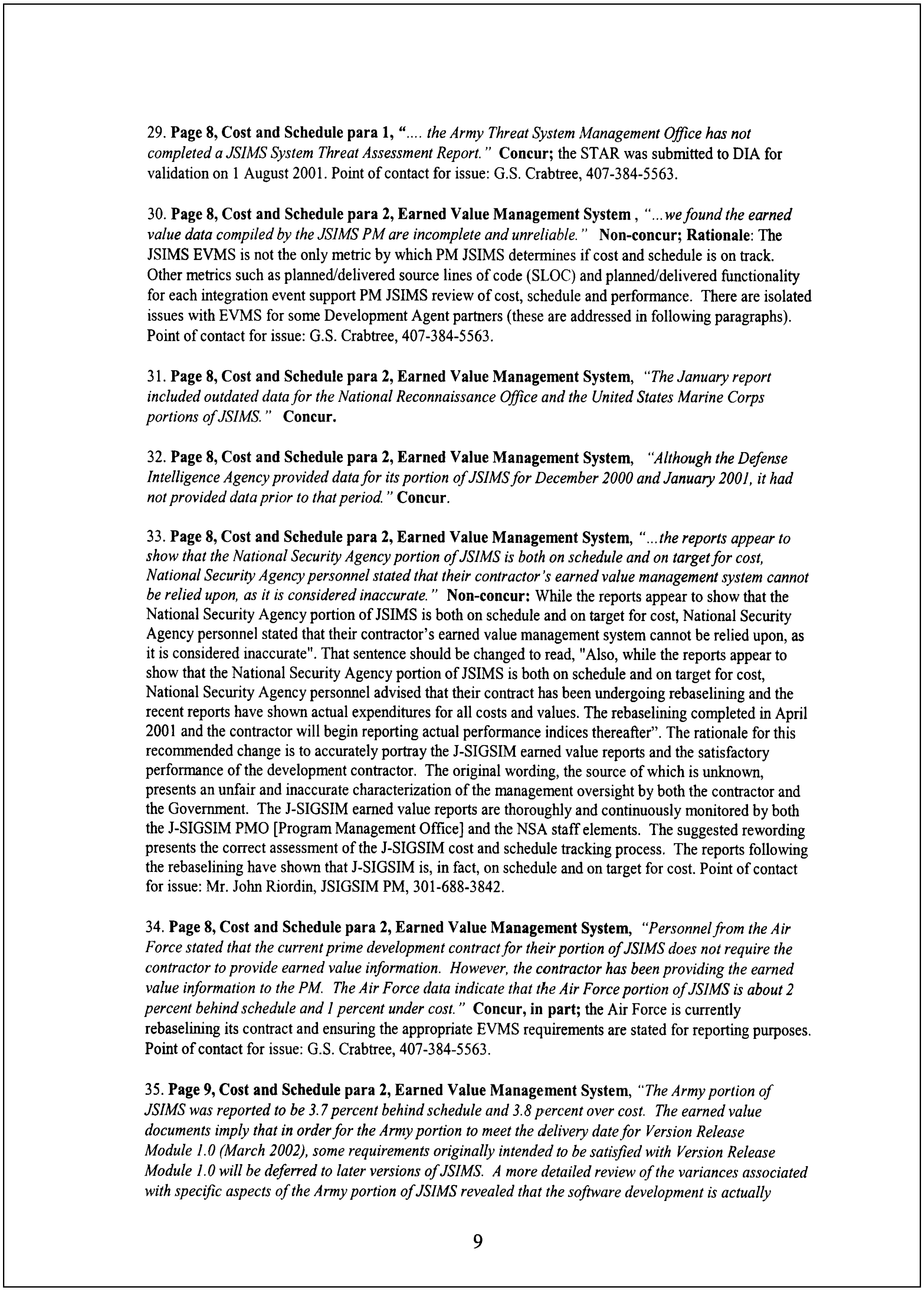
Pg 7 25. **Page 7/8, JSIMS Information Technology Security Certification and Accreditation para 5, Certification and Accreditation for the Common Component Workstation.** *"The National Reconnaissance Office is developing a user interface tool that will allow secure operations if the Common Component Workstation does not receive accreditation. They are coordinating the development with the Warfighters' Simulation Intelligence Module and the Defense Intelligence Agency Object Oriented Model of Intelligence Operations. Personnel within the National Reconnaissance Office stated that they developed the user interface tool because they have no confidence that the Common Component Workstation will be certified by Version Release Module 1."* **Concur.**

Pg 7 26. **Page 8, Cost and Schedule para 1, "***We determined that the JSIMS Earned Value Management System does not provide management with adequate cost and schedule information."* **Non-concur;** Rationale: The JSIMS EVMS is augmented by other data to support the PM JSIMS in determining if cost and schedule are on track. Other metrics such as planned/delivered Source Lines of Code (SLOC) and planned/delivered functionality for each integration event support PM JSIMS review of cost, schedule and performance. There are isolated issues with EVMS for some Development Agent partners (these are addressed in following paragraphs). Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 7 27. **Page 8, Cost and Schedule para 1, "...***the JSIMS program office has not constructed complete life-cycle cost estimates....."* **Concur, in part**; The Life-Cycle Cost Estimate has undergone validation by the respective partner cost agency and the Joint Cost Position will be finalized following decisions regarding Army program development. The JCP is expected to be validated by the subsequent Cost Assessment by the OSD CAIG. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 7 28. Page 8, Cost and Schedule para 1, *"...not included additional security requirements and emerging requirements in the life-cycle cost estimates or budgets..."* **Non-concur; Rationale**: there are no known security requirements which are not currently funded per the JCP under review. The one remaining security issue being presented to the Army is funding for a development environment supporting JSIMS common components' development, specifically CCWS and SNE, to meet JSIMS security policies. This is part of the Army's rebaselining under review by Army leadership. As for emerging requirements, the JSIMS users consisting of the Services, Joint Commands and Intelligence Agencies have the ability to submit and/or update requirements for JSIMS. All requirements are reviewed and prioritized by the JSIMS Requirements Control Board (JRCB), consisting of the JSIMS Executive Agents, for each Version Release. The Joint Warfighting Center (JWFC) as the lead user advocate is blocking the ORD per the 10 June 01 DoD 5000.2R. This blocking process will define a set of capabilities that JSIMS needs to deliver to meet training, experimentation or other objectives. Each block will include thresholds and objectives. The JSIMS program is currently funded to meet the established thresholds for Blocks 1 and 2 with no known disconnects for Blocks 3 and beyond. As the users review each Block with its associated versions, the EAs prioritize system level requirements based on funding constraints for their own programs and for the priorities of the Common Components and Alliance Products (PM JSIMS funded development). The users may identify new requirements based on changes in missions and roles or other factors as deemed necessary to support the Warfighter (such as potential contingency scenarios or experimentation desires). These emerging requirements may or may not take precedence over existing ones. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Final Report Reference



Pg 7 — 29. **Page 8, Cost and Schedule para 1, "**.... *the Army Threat System Management Office has not completed a JSIMS System Threat Assessment Report."* **Concur;** the STAR was submitted to DIA for validation on 1 August 2001. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 8 — 30. **Page 8, Cost and Schedule para 2, Earned Value Management System** , *"...we found the earned value data compiled by the JSIMS PM are incomplete and unreliable."* **Non-concur; Rationale**: The JSIMS EVMS is not the only metric by which PM JSIMS determines if cost and schedule is on track. Other metrics such as planned/delivered source lines of code (SLOC) and planned/delivered functionality for each integration event support PM JSIMS review of cost, schedule and performance. There are isolated issues with EVMS for some Development Agent partners (these are addressed in following paragraphs). Point of contact for issue: G.S. Crabtree, 407-384-5563.

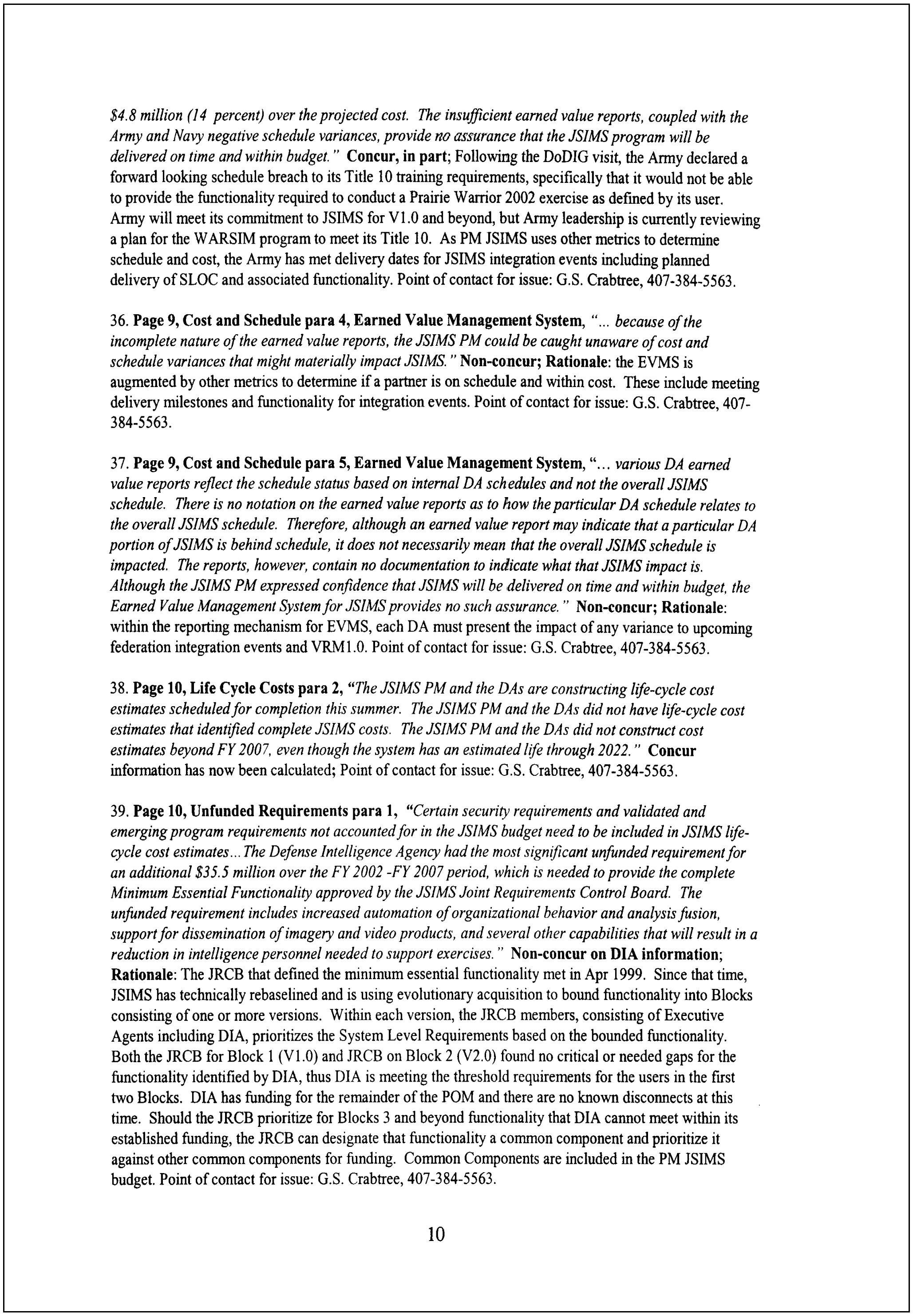
Pg 8 — 31. **Page 8, Cost and Schedule para 2, Earned Value Management System,** *"The January report included outdated data for the National Reconnaissance Office and the United States Marine Corps portions of JSIMS."* **Concur.**

Pg 8 — 32. **Page 8, Cost and Schedule para 2, Earned Value Management System,** *"Although the Defense Intelligence Agency provided data for its portion of JSIMS for December 2000 and January 2001, it had not provided data prior to that period."* **Concur**.

Revised Pg 8 — 33. **Page 8, Cost and Schedule para 2, Earned Value Management System,** *"...the reports appear to show that the National Security Agency portion of JSIMS is both on schedule and on target for cost, National Security Agency personnel stated that their contractor's earned value management system cannot be relied upon, as it is considered inaccurate."* **Non-concur:** While the reports appear to show that the National Security Agency portion of JSIMS is both on schedule and on target for cost, National Security Agency personnel stated that their contractor's earned value management system cannot be relied upon, as it is considered inaccurate". That sentence should be changed to read, "Also, while the reports appear to show that the National Security Agency portion of JSIMS is both on schedule and on target for cost, National Security Agency personnel advised that their contract has been undergoing rebaselining and the recent reports have shown actual expenditures for all costs and values. The rebaselining completed in April 2001 and the contractor will begin reporting actual performance indices thereafter". The rationale for this recommended change is to accurately portray the J-SIGSIM earned value reports and the satisfactory performance of the development contractor. The original wording, the source of which is unknown, presents an unfair and inaccurate characterization of the management oversight by both the contractor and the Government. The J-SIGSIM earned value reports are thoroughly and continuously monitored by both the J-SIGSIM PMO [Program Management Office] and the NSA staff elements. The suggested rewording presents the correct assessment of the J-SIGSIM cost and schedule tracking process. The reports following the rebaselining have shown that J-SIGSIM is, in fact, on schedule and on target for cost. Point of contact for issue: Mr. John Riordin, JSIGSIM PM, 301-688-3842.

Revised Pg 8 — 34. **Page 8, Cost and Schedule para 2, Earned Value Management System,** *"Personnel from the Air Force stated that the current prime development contract for their portion of JSIMS does not require the contractor to provide earned value information. However, the contractor has been providing the earned value information to the PM. The Air Force data indicate that the Air Force portion of JSIMS is about 2 percent behind schedule and 1 percent under cost."* **Concur, in part;** the Air Force is currently rebaselining its contract and ensuring the appropriate EVMS requirements are stated for reporting purposes. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 8 — 35. **Page 9, Cost and Schedule para 2, Earned Value Management System,** *"The Army portion of JSIMS was reported to be 3.7 percent behind schedule and 3.8 percent over cost. The earned value documents imply that in order for the Army portion to meet the delivery date for Version Release Module 1.0 (March 2002), some requirements originally intended to be satisfied with Version Release Module 1.0 will be deferred to later versions of JSIMS. A more detailed review of the variances associated with specific aspects of the Army portion of JSIMS revealed that the software development is actually*



$4.8 million (14 percent) over the projected cost. The insufficient earned value reports, coupled with the Army and Navy negative schedule variances, provide no assurance that the JSIMS program will be delivered on time and within budget." **Concur, in part**; Following the DoDIG visit, the Army declared a forward looking schedule breach to its Title 10 training requirements, specifically that it would not be able to provide the functionality required to conduct a Prairie Warrior 2002 exercise as defined by its user. Army will meet its commitment to JSIMS for V1.0 and beyond, but Army leadership is currently reviewing a plan for the WARSIM program to meet its Title 10. As PM JSIMS uses other metrics to determine schedule and cost, the Army has met delivery dates for JSIMS integration events including planned delivery of SLOC and associated functionality. Point of contact for issue: G.S. Crabtree, 407-384-5563.

36. **Page 9, Cost and Schedule para 4, Earned Value Management System**, *"... because of the incomplete nature of the earned value reports, the JSIMS PM could be caught unaware of cost and schedule variances that might materially impact JSIMS."* **Non-concur; Rationale**: the EVMS is augmented by other metrics to determine if a partner is on schedule and within cost. These include meeting delivery milestones and functionality for integration events. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 9

37. **Page 9, Cost and Schedule para 5, Earned Value Management System**, "*... various DA earned value reports reflect the schedule status based on internal DA schedules and not the overall JSIMS schedule. There is no notation on the earned value reports as to how the particular DA schedule relates to the overall JSIMS schedule. Therefore, although an earned value report may indicate that a particular DA portion of JSIMS is behind schedule, it does not necessarily mean that the overall JSIMS schedule is impacted. The reports, however, contain no documentation to indicate what that JSIMS impact is. Although the JSIMS PM expressed confidence that JSIMS will be delivered on time and within budget, the Earned Value Management System for JSIMS provides no such assurance."* **Non-concur; Rationale**: within the reporting mechanism for EVMS, each DA must present the impact of any variance to upcoming federation integration events and VRM1.0. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Revised
Pg 9

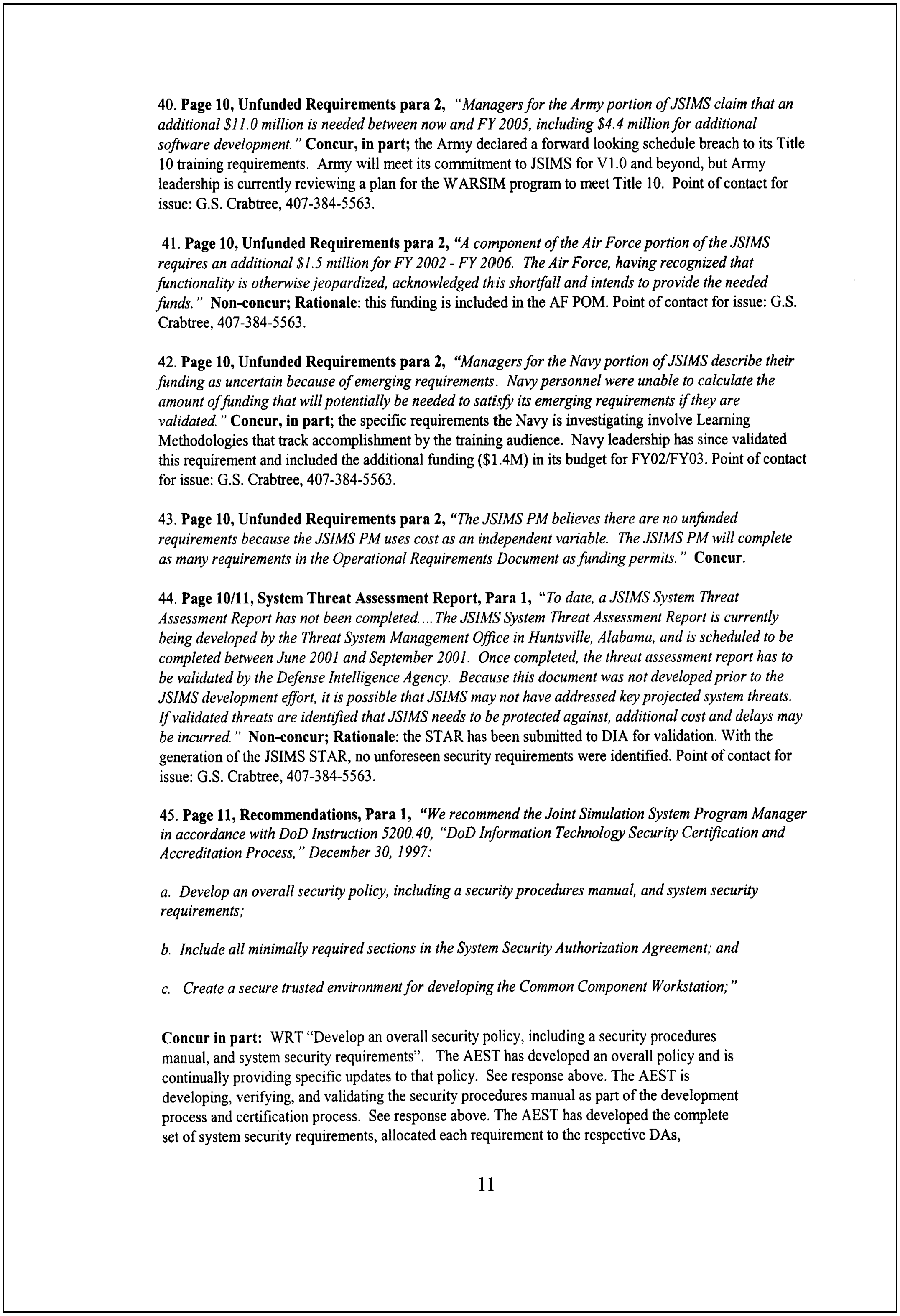
38. **Page 10, Life Cycle Costs para 2,** *"The JSIMS PM and the DAs are constructing life-cycle cost estimates scheduled for completion this summer. The JSIMS PM and the DAs did not have life-cycle cost estimates that identified complete JSIMS costs. The JSIMS PM and the DAs did not construct cost estimates beyond FY 2007, even though the system has an estimated life through 2022."* **Concur** information has now been calculated; Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 9

39. **Page 10, Unfunded Requirements para 1, "***Certain security requirements and validated and emerging program requirements not accounted for in the JSIMS budget need to be included in JSIMS life-cycle cost estimates... The Defense Intelligence Agency had the most significant unfunded requirement for an additional $35.5 million over the FY 2002 -FY 2007 period, which is needed to provide the complete Minimum Essential Functionality approved by the JSIMS Joint Requirements Control Board. The unfunded requirement includes increased automation of organizational behavior and analysis fusion, support for dissemination of imagery and video products, and several other capabilities that will result in a reduction in intelligence personnel needed to support exercises."* **Non-concur on DIA information**; **Rationale**: The JRCB that defined the minimum essential functionality met in Apr 1999. Since that time, JSIMS has technically rebaselined and is using evolutionary acquisition to bound functionality into Blocks consisting of one or more versions. Within each version, the JRCB members, consisting of Executive Agents including DIA, prioritizes the System Level Requirements based on the bounded functionality. Both the JRCB for Block 1 (V1.0) and JRCB on Block 2 (V2.0) found no critical or needed gaps for the functionality identified by DIA, thus DIA is meeting the threshold requirements for the users in the first two Blocks. DIA has funding for the remainder of the POM and there are no known disconnects at this time. Should the JRCB prioritize for Blocks 3 and beyond functionality that DIA cannot meet within its established funding, the JRCB can designate that functionality a common component and prioritize it against other common components for funding. Common Components are included in the PM JSIMS budget. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Revised
Pg 10

Final Report Reference



Pg 10

40. **Page 10, Unfunded Requirements para 2,** *"Managers for the Army portion of JSIMS claim that an additional $11.0 million is needed between now and FY 2005, including $4.4 million for additional software development."* **Concur, in part;** the Army declared a forward looking schedule breach to its Title 10 training requirements. Army will meet its commitment to JSIMS for V1.0 and beyond, but Army leadership is currently reviewing a plan for the WARSIM program to meet Title 10. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 10

41. **Page 10, Unfunded Requirements para 2,** *"A component of the Air Force portion of the JSIMS requires an additional $1.5 million for FY 2002 - FY 2006. The Air Force, having recognized that functionality is otherwise jeopardized, acknowledged this shortfall and intends to provide the needed funds."* **Non-concur; Rationale**: this funding is included in the AF POM. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 10

42. **Page 10, Unfunded Requirements para 2,** *"Managers for the Navy portion of JSIMS describe their funding as uncertain because of emerging requirements. Navy personnel were unable to calculate the amount of funding that will potentially be needed to satisfy its emerging requirements if they are validated."* **Concur, in part**; the specific requirements the Navy is investigating involve Learning Methodologies that track accomplishment by the training audience. Navy leadership has since validated this requirement and included the additional funding ($1.4M) in its budget for FY02/FY03. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 10

43. **Page 10, Unfunded Requirements para 2,** *"The JSIMS PM believes there are no unfunded requirements because the JSIMS PM uses cost as an independent variable. The JSIMS PM will complete as many requirements in the Operational Requirements Document as funding permits."* **Concur.**

Pg 10

44. **Page 10/11, System Threat Assessment Report, Para 1,** *"To date, a JSIMS System Threat Assessment Report has not been completed.... The JSIMS System Threat Assessment Report is currently being developed by the Threat System Management Office in Huntsville, Alabama, and is scheduled to be completed between June 2001 and September 2001. Once completed, the threat assessment report has to be validated by the Defense Intelligence Agency. Because this document was not developed prior to the JSIMS development effort, it is possible that JSIMS may not have addressed key projected system threats. If validated threats are identified that JSIMS needs to be protected against, additional cost and delays may be incurred."* **Non-concur; Rationale**: the STAR has been submitted to DIA for validation. With the generation of the JSIMS STAR, no unforeseen security requirements were identified. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Revised
Pg 12

45. **Page 11, Recommendations, Para 1,** *"We recommend the Joint Simulation System Program Manager in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997:*

a. Develop an overall security policy, including a security procedures manual, and system security requirements;

b. Include all minimally required sections in the System Security Authorization Agreement; and

c. Create a secure trusted environment for developing the Common Component Workstation;"

Concur in part: WRT "Develop an overall security policy, including a security procedures manual, and system security requirements". The AEST has developed an overall policy and is continually providing specific updates to that policy. See response above. The AEST is developing, verifying, and validating the security procedures manual as part of the development process and certification process. See response above. The AEST has developed the complete set of system security requirements, allocated each requirement to the respective DAs,

11

Final Report Reference

sequenced those requirements to FIEs, and baselined those requirements via the JCCB. See response above. WRT "Include all minimally required sections in the System Security Authorization Agreement." The AEST has developed the SSAA in accordance with the DoDIIS-Tailored SSAA guidelines contained in the *DODIIS Security Certification and Accreditation Guide*, DS-2610-142-01, dated April 2001. All information required by the DITSCAP is included in the DoDIIS-Tailored SSAA as explained in response above. The JSIMS System DAA agrees with this format. WRT "Create a secure trusted environment for developing the Common Component Workstation." The Land Component of JSIMS is requesting funding to correct the CCWS development environment. See response above. Estimated completion date (ECD) for on-going actions: 15 Feb 2002; Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

46. **Page 11, Recommendations, Para 2,** *"We recommend the Joint Simulation System Program Manager in accordance with DoD Regulation 5000.2-R (Interim) "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems Acquisitions Programs," January 4, 2001:* Pg 12

a. Require Development Agents to provide complete earned value information; and

b. Construct complete life-cycle cost estimates that include requirements for which funding has not been established." **Concur**; see preceding paragraphs on EVMS and LCCE. Point of contact for issue: G.S. Crabtree, 407-384-5563.

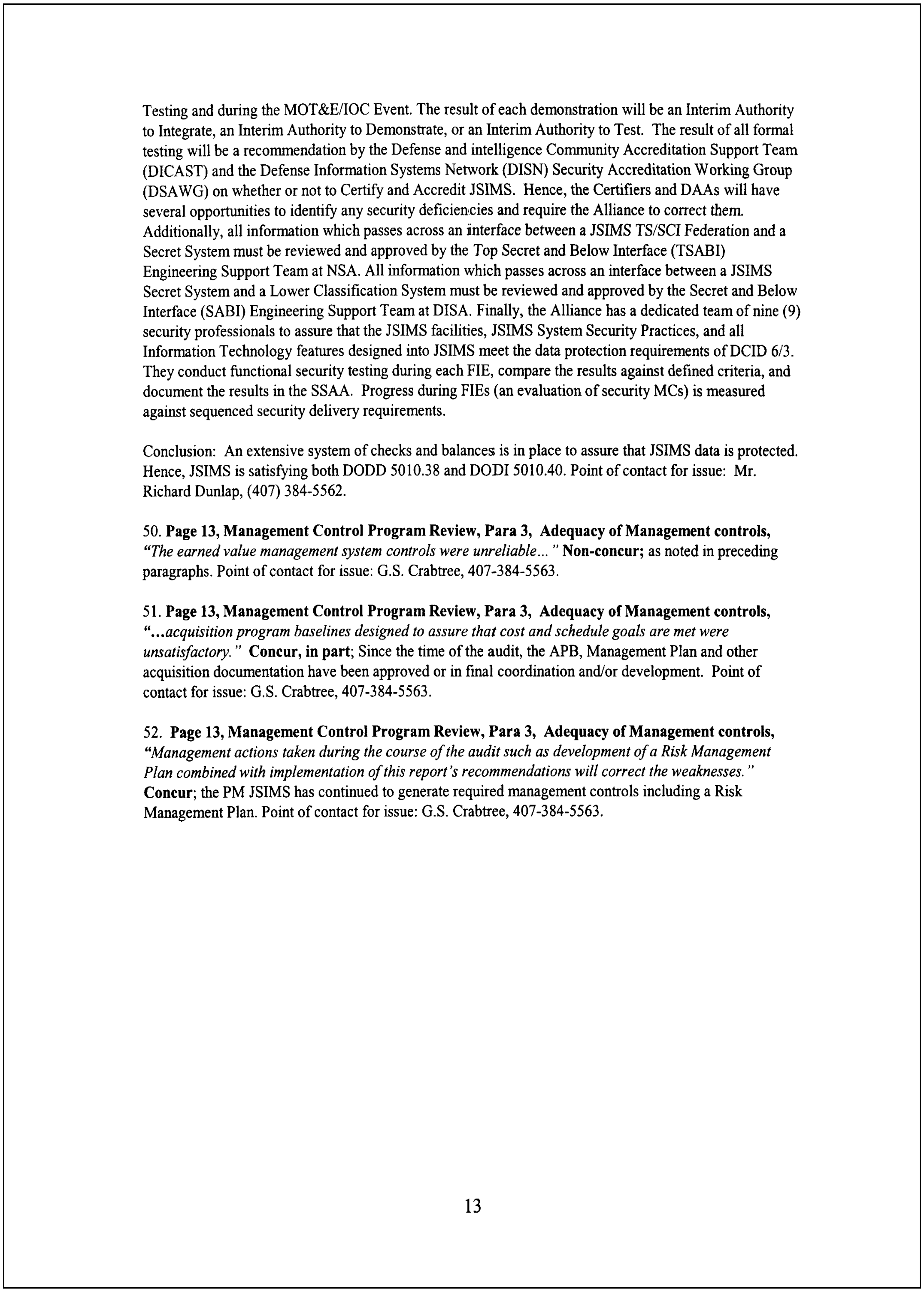
47. **Page 13, Management Control Program Review, Para 2, Scope of the Review of the Management Control Program.** *"For the JSIMS program, we reviewed the plan for Internal Management and Control of Funds and management self-evaluation. Management's self-evaluation had uncovered weaknesses prior to our audit, and management had taken corrective action;* **Concur.** Pg 14

48. Page 13, Management Control Program Review, Para 3, Adequacy of Management controls, *"We identified material management control weaknesses as defined in DoD Instruction 5010.40. ..."* **Non-concur;** see discussions on Earned value and security control programs in-place. Point of contact for issue: G.S. Crabtree, 407-384-5563.49. Pg 14

Page 13, Management Control Program Review, Para 3, Adequacy of Management controls, "System security controls were incomplete." **Non-Concur**; **Rationale**: DoD Instruction 5010.40, E4.1.9, states that Security MCs must include "...safeguarding classified resources but not peripheral assets and support functions covered by other reporting categories. Also covers the DoD programs for protection of classified information." Hence, the MC for security must assure that classified data and systems containing the classified data are protected. Pg 14

DoD Directive 5010.38, 4.2.4, states "Wherever possible and to the greatest extent possible, rely on organizationally required or other contributing information sources (such as management and oversight reviews, computer security reviews, financial system reviews, audits, inspections, investigations, internal review studies, quality management initiatives, and management and/or consulting reviews). MC Program evaluation should not cause the duplication of existing information that pertains to assessing the effectiveness of MCs or information that may be used for that purpose." Hence, JSIMS is authorized to use existing procedures for Security MC if those processes cover the full scope of protecting JSIMS data and the systems containing that data. JSIMS protects classified data IAW governing regulations and directives. Adherence to those regulations and directives is continuously reviewed throughout the JSIMS development cycle by independent agencies and evaluators. More specifically, during the development process, the JSIMS facility and system security features will be demonstrated to the Certifiers and DAAs prior to each FIE (FIE 3, 4, and 5), prior to System Test, and prior to each major user event (SFA, PW02, MOT&E). Additionally, the Certifiers and DAAs conduct formal Information Assurance testing during System

Final Report Reference



Testing and during the MOT&E/IOC Event. The result of each demonstration will be an Interim Authority to Integrate, an Interim Authority to Demonstrate, or an Interim Authority to Test. The result of all formal testing will be a recommendation by the Defense and intelligence Community Accreditation Support Team (DICAST) and the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) on whether or not to Certify and Accredit JSIMS. Hence, the Certifiers and DAAs will have several opportunities to identify any security deficiencies and require the Alliance to correct them. Additionally, all information which passes across an interface between a JSIMS TS/SCI Federation and a Secret System must be reviewed and approved by the Top Secret and Below Interface (TSABI) Engineering Support Team at NSA. All information which passes across an interface between a JSIMS Secret System and a Lower Classification System must be reviewed and approved by the Secret and Below Interface (SABI) Engineering Support Team at DISA. Finally, the Alliance has a dedicated team of nine (9) security professionals to assure that the JSIMS facilities, JSIMS System Security Practices, and all Information Technology features designed into JSIMS meet the data protection requirements of DCID 6/3. They conduct functional security testing during each FIE, compare the results against defined criteria, and document the results in the SSAA. Progress during FIEs (an evaluation of security MCs) is measured against sequenced security delivery requirements.

Conclusion: An extensive system of checks and balances is in place to assure that JSIMS data is protected. Hence, JSIMS is satisfying both DODD 5010.38 and DODI 5010.40. Point of contact for issue: Mr. Richard Dunlap, (407) 384-5562.

Pg 14

50. **Page 13, Management Control Program Review, Para 3, Adequacy of Management controls,** *"The earned value management system controls were unreliable..."* **Non-concur;** as noted in preceding paragraphs. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 14

51. **Page 13, Management Control Program Review, Para 3, Adequacy of Management controls,** *"...acquisition program baselines designed to assure that cost and schedule goals are met were unsatisfactory."* **Concur, in part**; Since the time of the audit, the APB, Management Plan and other acquisition documentation have been approved or in final coordination and/or development. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Pg 14

52. **Page 13, Management Control Program Review, Para 3, Adequacy of Management controls,** *"Management actions taken during the course of the audit such as development of a Risk Management Plan combined with implementation of this report's recommendations will correct the weaknesses."* **Concur**; the PM JSIMS has continued to generate required management controls including a Risk Management Plan. Point of contact for issue: G.S. Crabtree, 407-384-5563.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary Ugone
Charles Santoni
Sean Mitchell
Averel Gregg
John Mitton
Patricia Joyner
David Huff
Bridget Yakley